



CJCSM 6510.01  
25 March 2003  
CH 1 10 August 2004

# **DEFENSE-IN-DEPTH: INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)**



**JOINT STAFF  
WASHINGTON, D.C. 20318**

(INTENTIONALLY BLANK)



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

---

J6  
DISTRIBUTION: A, B, C, J and S

CJCSM 6510.01  
25 March 2003  
CH 1 10 August 2004

DEFENSE-IN-DEPTH: INFORMATION ASSURANCE (IA) AND COMPUTER  
NETWORK DEFENSE (CND)

References: See Enclosure D.

1. Purpose. This manual provides guidance and procedures for implementing the IA defense-in-depth strategy and standards. The mix of safeguards selected for an information system processing classified or sensitive-but-unclassified information will ensure the information system meets minimum requirements set forth in this manual. Minimum requirements will be met through automated and manual means in a cost-effective, integrated manner. The element of defense-in-depth focuses on three major areas:

- a. People.
- b. Operations.
- c. Defense of the information environment, including:
  - (1) The computing environment.
  - (2) The network.
  - (3) The enclave boundary.
  - (4) The supporting infrastructures.

2. Applicability. This manual applies to the Joint Staff, Services, combatant commands, Defense agencies, DOD field activities, and joint and combatant activities.

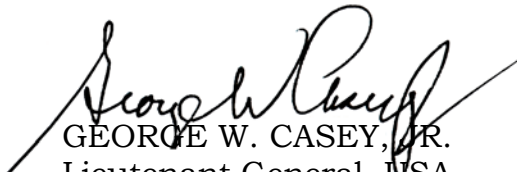
3. Procedures. See Enclosures A, B, and C.

**FOR OFFICIAL USE ONLY**

4. Releasability. This manual is approved for limited release. DOD components (to include the combatant commands) and other Federal agencies may obtain copies of this manual through controlled Internet access only (limited to .mil and .gov users) from the CJCS Directives Home Page--<http://www.dtic.mil/doctrine>. Joint Staff activities may access or obtain copies of this instruction/manual/notice from the Joint Staff LAN.

5. Effective Date. This manual is effective immediately.

For the Chairman of the Joint Chiefs of Staff:



GEORGE W. CASEY, JR.  
Lieutenant General, USA  
Director, Joint Staff

Enclosures:

- A - Defense-in-Depth – People
- B - Defense-in-Depth – Operations
- C - Defense-in-Depth – Defending the Information Environment
- D - References
- Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
Secretary of Defense .....	2
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) .....	2

(INTENTIONALLY BLANK)

# LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSM 6510.01. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-G-1 thru C-G-2	O
i thru xiv	1	C-G-A-1 thru C-G-A-4	O
A-1 thru A-2	O	C-G-B-1 thru C-G-B-4	O
A-A-1 thru A-A-18	O	C-G-C-1 thru C-G-C-2	O
A-B-1 thru A-B-38	O	C-G-D-1 thru C-G-D-6	O
A-C-1 thru A-C-2	O	C-H-1 thru C-H-10	O
B-1 thru B-2	O	C-I-1 thru C-I-8	O
B-A-1 thru B-A-22	1	C-I-A-1 thru C-I-A-6	O
B-B-1 thru B-B-16	O	C-I-B-1 thru C-I-B-4	O
B-C-1 thru B-C-4	O	C-J-1 thru C-J-14	O
B-D-1 thru B-D-10	O	C-K-1 thru C-K-6	O
B-E-1 thru B-E-2	O	C-K-A-1 thru C-K-A-6	O
C-1 thru C-32	O	C-L-1 thru C-L-2	O
C-A-1 thru C-A-6	O	C-M-1 thru C-M-2	O
C-B-1 thru C-B-14	O	C-N-1 thru C-N-8	O
C-C-1 thru C-C-2	O	C-O-1 thru C-O-8	O
C-D-1 thru C-D-6	O	C-P-1 thru C-P-2	O
C-E-1 thru C-E-12	O	D-1 thru D-6	O
C-F-1 thru C-F-2	O	GL-1 thru GL-34	O

(INTENTIONALLY BLANK)



## RECORD OF CHANGES

[illegible]

(INTENTIONALLY BLANK)



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF NOTICE

J6

DISTRIBUTION: A, B, C, J

CJCSM 6510.01 CH 1

10 August 2004

## CHANGE 1 TO CJCS MANUAL 6510.01

1. Holders of CJCSM 6510.01, 25 March 2003, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," are requested to make the following changes:

### Page Substitution

#### Remove Page(s)

B-A-1 to B-A-26

#### Add Page(s)

B-A-1 to B-A-22

2. Summary of the changes is as follows: Replace Appendix A to Enclosure B, "INFORMATION ASSURANCE VULNERABILITY MANAGEMENT PROGRAM."

3. When the prescribed action has been taken, this transmittal should be filed behind the record of changes page in the basic document.

4. This manual is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this notice through the Internet from the CJCS Directives Home Page--  
[http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives). Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

A handwritten signature in black ink, reading "Michael D. Maples".

MICHAEL D. MAPLES  
Major General, USA  
Vice Director, Joint Staff

Enclosure(s):

A – Information Assurance Vulnerability Management Program

## TABLE OF CONTENTS

	Page
ENCLOSURE	
A DEFENSE-IN-DEPTH - PEOPLE .....	A-1
APPENDIX A INDIVIDUAL FUNCTIONS AND RESPONSIBILITIES	
General .....	A-A-1
Designated Approving Authority .....	A-A-1
Information Assurance Manager .....	A-A-4
Information Assurance Officer .....	A-A-6
System Administrators .....	A-A-7
Program Managers, Certification Authorities, and User Representatives .....	A-A-9
Individuals and Information System Users.....	A-A-11
Network Suspensions .....	A-A-13
User Agreement.....	A-A-13
APPENDIX B TRAINING, EDUCATION, AND CERTIFICATION	
General.....	A-B-1
DOD Training and Certification Objectives.....	A-B-1
IA and Information System Security .....	A-B-2
Training, Education and Certification .....	A-B-2
Minimum User IA Training and Awareness .....	A-B-3
SA Certification .....	A-B-5
SA Certification Requirements .....	A-B-6
Skill Level 1 SA .....	A-B-6
Skill Level 2 SA .....	A-B-12
Skill Level 3 SA .....	A-B-22
Additional IA Professionals .....	A-B-29
APPENDIX C IA ORGANIZATIONS ROLES AND MISSIONS - TO BE PUBLISHED (TBP).....	A-C-1
B DEFENSE-IN-DEPTH - OPERATIONS .....	B-1
APPENDIX A INFORMATION ASSURANCE VULNERABILITY MANAGEMENT PROGRAM	
IAVM Program .....	B-A-1
Applicability and Scope .....	B-A-1
Individual and Organization Accountability for Implementing IAVM.....	B-A-2
IAVM Asset Compliance Status.....	B-A-2

Organization Responsibilities.....	B-A-3
Individual Responsibilities .....	B-A-7
IAVM Vulnerability Notifications .....	B-A-10
IAVM Program Process Flow .....	B-A-12
Operating NonCompliant Assets Accountability and Responsibilities .....	B-A-18
USSTRATCOM IAVA Compliance and Network Status Oversight .....	B-A-19
Component NonCompliance Notification and Enforcement Procedures.....	B-A-19
IAVM Program Compliance Validation and Verification.....	B-A-20
Incident and Follow-Up Reporting.....	B-A-21
Vulnerability Management System (VMS)/Vulnerability Compliance Tracking System (VCTS).....	B-A-22

#### APPENDIX B INCIDENT AND VULNERABILITY REPORTING

Incident and Vulnerability Reporting .....	B-B-1
Incident Reporting Procedures.....	B-B-2
Vulnerability Analysis.....	B-B-13
Incident and Vulnerability Feedback Methods .....	B-B-14

#### APPENDIX C INFORMATION OPERATIONS CONDITIONS

Introduction .....	B-C-1
Purpose .....	B-C-1
Applicability .....	B-C-1
Authority .....	B-C-1
Description.....	B-C-2
Assumptions .....	B-C-3
INFOCON Structure .....	B-C-3
Support.....	B-C-4

#### APPENDIX D JOINT INFORMATION ASSURANCE RED TEAM OPERATIONS

Purpose.....	B-D-1
General .....	B-D-1
Considerations and Guidelines for IA Red Team Operations .....	B-D-3
Support.....	B-D-9

APPENDIX E	IA INTEGRATION INTO JOINT PLANS AND PLANNING (TBP).....	B-E-1
C	DEFENSE-IN-DEPTH – DEFENDING THE INFORMATION ENVIRONMENT	
	Defense-in-Depth.....	C-1
	Defending the Computing Environment.....	C-1
	Defending the Network.....	C-5
	Defending the Enclave Boundary .....	C-15
	Establish Supporting Infrastructure.....	C-20
	Defense-in-Depth Examples .....	C-21
	Guidance .....	C-31
APPENDIX A	AUTHENTICATION	
	Authentication .....	C-A-1
	System Access.....	C-A-1
	Password Ownership .....	C-A-1
	Password Format.....	C-A-1
	User Validation .....	C-A-2
	Password Protection .....	C-A-2
	User Maintenance .....	C-A-2
	Storage.....	C-A-2
	Authentication Failures .....	C-A-3
	User Password History .....	C-A-4
	Memorizing Passwords .....	C-A-4
	Disclosure of Passwords .....	C-A-4
	Compromised Passwords .....	C-A-5
	Unclassified System Access .....	C-A-5
	Classified System Access .....	C-A-5
	Factory-Issued Identifiers or Passwords.....	C-A-5
	Conditions Requiring Password Changes .....	C-A-5
	Disabling Accounts.....	C-A-6
	Classification and Control of Passwords .....	C-A-6
APPENDIX B	FOREIGN ACCESS TO DOD INFORMATION AND INFORMATION SYSTEMS	
	Procedures .....	C-B-1
	Foreign National Access to Information.....	C-B-1
	Assignment of Foreign Nationals to DOD Organizations.....	C-B-2
	Interconnections to Agencies of Foreign Governments.....	C-B-3

Page

Foreign National Individual Access to Unclassified DOD Information Systems .....	C-B-5
Foreign National Access to Classified Information Systems .....	C-B-7
DOD Foreign National Employees and Foreign National Service Members as Authorized Users .....	C-B-9
DOD Foreign National Contractors .....	C-B-10
Foreign National in IT Position.....	C-B-11
Release of USG INFOSEC Products or Associated INFOSEC Information to Foreign Governments .....	C-B-11

APPENDIX C ELECTRONIC NOTICE AND CONSENT BANNER.....	C-C-2
---	-------

APPENDIX D PHYSICAL AND ENVIRONMENTAL SECURITY Description.....	C-D-1
Physical Security Programs .....	C-D-2
Physical Security Planning .....	C-D-2
Security System Level and Mission Category.....	C-D-3
Fire-Safety Factors .....	C-D-4
Failure of Supporting Infrastructure .....	C-D-5
Plumbing Leaks.....	C-D-5

APPENDIX E HANDLING, MARKING, AND LABELING INFORMATION AND THE PROTECTION OF CLASSIFIED AND UNCLASSIFIED NATIONAL SECURITY-RELATED INFORMATION Handling, Marking, and Labeling Information...	C-E-1
Protecting Unclassified National Security- Related Telecommunications Information .....	C-E-3

APPENDIX F DEFENDING BACKBONE NETWORKS Backbone Networks.....	C-F-1
Access Controls.....	C-F-1
Authentication .....	C-F-1
Confidentiality.....	C-F-1
Integrity .....	C-F-2
Nonrepudiation .....	C-F-2



APPENDIX G	COMMUNICATIONS SECURITY	
	COMSEC Material Control System.....	C-G-1
	Granting Access to US Classified	
	Cryptographic Information .....	C-G-1
	Release of COMSEC Information to US	
	Nongovernmental Sources .....	C-G-1
	Disclosure or Release of COMSEC Information	
	to Foreign Governments and International	
	Organizations .....	C-G-1
	COMSEC Monitoring .....	C-G-1
ANNEX A	CRYPTOGRAPHIC ACCESS CRITERIA	
	Access Requirements.....	C-G-A-1
	Procedures .....	C-G-A-1
	Exceptions .....	C-G-A-2
	Sample Cryptographic Access Briefing .....	C-G-A-2
ANNEX B	RELEASE OF COMSEC INFORMATION TO US	
	CONTRACTORS AND OTHER US	
	NONGOVERNMENTAL ORGANIZATIONS OR	
	PERSONS	
	General .....	C-G-B-1
	Standards and Procedures .....	C-G-B-1
	Criteria.....	C-G-B-1
	Responsibilities .....	C-G-B-2
	Exceptions .....	C-G-B-2
ANNEX C	DISCLOSURE OR RELEASE OF COMSEC	
	INFORMATION TO FOREIGN GOVERNMENTS AND	
	INTERNATIONAL ORGANIZATIONS	
	General .....	C-G-C-1
	Information Request Requirements.....	C-G-C-1
	Validation.....	C-G-C-2
ANNEX D	COMSEC MONITORING	
	General .....	C-G-D-1
	Guidelines for the Conduct of COMSEC	
	Monitoring .....	C-G-D-2
	Control of Monitoring Records and	
	Equipment .....	C-G-D-4

Joint COMSEC Monitoring Support .....	C-G-D-5
---------------------------------------	---------

## APPENDIX H PROTECTION MECHANISMS - LEVELS OF CONCERN AND ROBUSTNESS

Levels of Concern .....	C-H-1
Levels of Robustness .....	C-H-2
Security Services Robustness .....	C-H-5
Access Control Robustness.....	C-H-5
Encryption .....	C-H-8
Cryptographic Functions .....	C-H-9

## APPENDIX I INTERCONNECTION AND DATA TRANSFER BETWEEN SECURITY DOMAINS

Description.....	C-I-1
Background .....	C-I-1
DITSCAP Procedure for Interconnections of Security Domains.....	C-I-2
Procedures for Data Transfer Across Security Domains .....	C-I-7

## ANNEX A INTERDOMAIN DATA TRANSFER - GENERIC FRAMEWORK AND SCENARIO

Generic Framework and Scenario .....	C-I-A-1
Interdomain Transfer Scenario .....	C-I-A-3

## ANNEX B CONTROLLED INTERFACE CHARACTERISTICS

Controlled Interface Overview .....	C-I-B-1
Common Controlled Interface Requirements...	C-I-B-1
Controlled Interface Confidentiality Requirements.....	C-I-B-2
Controlled Interface Integrity Requirements....	C-I-B-3

## APPENDIX J MOBILE CODE

Purpose.....	C-J-1
Background .....	C-J-1
Definitions .....	C-J-1
Scope .....	C-J-5
Guidance for Category 1 Mobile Code Technologies .....	C-J-5
Mobile Code in E-mail Messages and Attachments .....	C-J-7

Guidance for Category 2 Mobile Code Technologies .....	C-J-9
Workstation Guidance to Disable Category 2 Mobile Code Technologies .....	C-J-11
Guidance for Category 3 Mobile Code Technologies .....	C-J-12
Emerging Technologies .....	C-J-12
Guidance to Developers on Selection and Use of Mobile Code in DOD Information Systems .....	C-J-12

#### APPENDIX K FIREWALL GUIDANCE

Background .....	C-K-1
Objective .....	C-K-2
Security Policy .....	C-K-2
Firewall Implementation .....	C-K-3
Firewall Security Requirements .....	C-K-3
Configuration Management, Maintenance, and Testing of Firewall .....	C-K-5
Scope .....	C-K-6
Overview .....	C-K-7
Firewall Technology Types .....	C-K-9
Example Firewall Architectures .....	C-K-11
Firewall Placement .....	C-K-14
Firewall Functions .....	C-K-15
Potential Attacks .....	C-K-18

#### ANNEX A ROBUSTNESS

Robustness Strategy .....	C-K-A-1
Determining the Degree of Robustness .....	C-K-A-1

#### APPENDIX L PORTS AND PROTOCOLS MANAGEMENT

PROCESS (TBP) .....	C-L-1
---------------------	-------

#### APPENDIX M VIRTUAL PRIVATE NETWORKS (TBP) .....

C-M-1

#### APPENDIX N INTRUSION DETECTION SYSTEM

Description .....	C-N-1
Information System and the IDS .....	C-N-3
Potential Attacks .....	C-N-3

	Page
Considerations in Selecting an IDS.....	C-N-4
Minimum Security Functions and Requirements .....	C-N-6
Additional Information.....	C-N-7
APPENDIX O PUBLIC KEY MANAGEMENT	
Public Key Infrastructure .....	C-O-1
Public Key Certificates.....	C-O-2
General Usage .....	C-O-3
Potential Attacks .....	C-O-5
PKI Authorities and Functions.....	C-O-6
Additional Information.....	C-O-8
APPENDIX P SYSTEM SECURITY AUTHORIZATION	
AGREEMENT (TBP) .....	C-P-1
D REFERENCES.....	D-1
GLOSSARY	
PART I – ABBREVIATIONS AND ACRONYMS.....	GL-1
PART II –DEFINITIONS.....	GL-7
FIGURE	
B-A-1 Vulnerability Notice Number Format .....	B-A-12
B-A-3 Reporting Chain of Command.....	B-A-16
B-A-4 Compliance Data.....	B-A-17
B-B-1 Incident Reporting Structure .....	B-B-3
B-B-2 Reportable Incident and Event Priorities.....	B-B-5
C-1 Computing Environment .....	C-2
C-2 Defending the Network and Infrastructure.....	C-6
C-3 Defending the Enclave Boundary.....	C-15
C-4 Typical RASP Configuration.....	C-30
C-C-1 Example of Notice and Consent Banner .....	C-C-1
C-D-1 Security System Level and Mission Category.....	C-D-4
C-G-B-1 Checklist for Preparing Exception Requests.....	C-G-B-3
C-I-A-1 Generic Framework for Inter-Domain Transfer.....	C-I-A-1
C-I-A-2 Example Automated Transfer Process.....	C-I-A-4
C-K-1 Basic Filter (Screening Router) .....	C-K-11
C-K-2 Dual-Homed.....	C-K-12
C-K-3 Screened Host .....	C-K-13
C-K-4 Dual-Homed with Screened Subnet (DMZ).....	C-K-14

C-K-A-1	Determining the Level of Robustness Flow Chart .....	C-K-A-1
C-N-1	Intrusion Detection System .....	C-N-1

## TABLE

A-B-1	Skill Level 1 Requirements .....	A-B-7
A-B-2	Skill Level 2 Requirements .....	A-B-13
A-B-3	Skill Level 3 Requirements .....	A-B-23
A-B-4	IAO Training Standards.....	A-B-31
A-B-5	IAM Training Standards .....	A-B-33
A-B-6	DAA Training Standards.....	A-B-35
B-B-1	Reporting Methods .....	B-B-6
B-B-2	Incident Categories.....	B-B-7
B-B-3	Incident Reporting Timelines .....	B-B-9
B-B-4	Incident Report Format .....	B-B-10
C-E-1	Information Guide for Protecting Unclassified National Security-Related Telecommunications Information .....	C-E-4
C-H-1	Security Services Robustness .....	C-H-1
C-H-2	Access Control Robustness Examples.....	C-H-6
C-H-3	Data Encryption Robustness .....	C-H-9
C-H-4	Algorithm Robustness Examples .....	C-H-10
C-O-1	General Usage .....	C-O-5

(INTENTIONALLY BLANK)

## ENCLOSURE A

### DEFENSE-IN-DEPTH – PEOPLE

#### INTRODUCTION

1. People, using technologies to conduct operations, are the central element of defense-in-depth. It takes people to design, build, test, install, operate, evaluate, and maintain protection mechanisms.
2. The best talent available must be recruited and wisely assigned. Also needed is a highly reliable personnel security system of appropriate background investigations, security clearances, credentials, and attention to suspicious actions that ensure only trustworthy persons have access. In modern defense forces, individual contributions must be integrated into larger coordinated team and organization efforts. Command attention, positive involvement, and leadership are vital at all levels of organization.
3. Every person who uses or manages information systems (military, government civilian, contractor and foreign national) has a responsible security role. Key roles and responsibilities are outlined in Appendix A of this enclosure and include the system administrator (SA), information assurance manager (IAM), information assurance office (IAO), designated approving authority (DAA), and end-user.
4. To gain and maintain the knowledge and expertise to perform these vital tasks, a comprehensive program of education, training, practical experience, and awareness is needed. Professionalization and certification can increase motivation and provide a validated and recognized expert cadre. Appendix B of this enclosure, "Training, Education, and Certification," outlines basic information assurance (IA) standards for SAs and information system users (military, government civilian, contractor, and foreign national).
5. Appendix C will be published during next change to manual.

(INTENTIONALLY BLANK)



## APPENDIX A TO ENCLOSURE A

### INDIVIDUAL FUNCTIONS AND RESPONSIBILITIES

1. General. All DOD activities must ensure their systems are administered by technically qualified personnel who are provided periodic professional training in system administration and IA as well as the necessary tools to assist in effective baseline management, auditing, and network intrusion detection. Configuration management, proper staffing, and strong systems policies are critical to reliable and secure operations. To accomplish this, the following key IA functions and responsibilities will be conducted by the DAA, IAM, IAO, SA, and individual users as outlined in this appendix.

2. Designated Approving Authority

a. The DAA will be a US citizen.

b. The DAA will be an employee of the US Government (USG) (minimum grade of O-6/GS-15), will comply with the security requirements of DOD 5200.2-R (reference a), and hold USG security clearance (e.g., TOP SECRET) and access approvals commensurate with all information systems under the DAA's jurisdiction.

c. The DAA will have a level of authority commensurate with accepting, in writing, the risk of operating all information systems under the DAA's jurisdiction. The appointing authority will ensure that individuals knowledgeable in all areas of security are available to support the DAA so that a technically correct assessment of the security characteristics of the information system can be made.

d. The DAA will understand the operational need for the system(s) and the operational consequences of not operating the system(s). The DAA will have an in-depth knowledge of Defense in Depth to drive state of the art acquisition, focus a robust training program, and institute executable policy across the IA enterprise.

e. The DAA will execute the following responsibilities:

(1) Ensure a properly conducted certification is accomplished on each system considered for accreditation in accordance with DOD Information Technology Security Certification and Accreditation Process (DITSCAP).

(2) Issue a written accreditation statement after formal review of the system security authorization agreement (SSAA), including the certification report issued by the certification authority (CA).

(3) Grant final and interim accreditation of a network or system in a specified security mode.

(4) Ensure that security is incorporated as an element of the information system life-cycle process.

(5) Delegate accreditation approval authority if necessary or desirable. The individual(s) delegated must be at least an O-6 or GS-15 and in an IA or information system security position to be granted this authority and meet the requirements specified in paragraph 2.b. above. Delegation of authority must be in writing and include the responsibility to implement countermeasures to maintain an acceptable level of risk or shut down system operations.

(6) Review the SSAA to confirm that the residual risk is within acceptable limits.

(7) Verify that each SSAA complies with information system security requirements as reported by the IAM. Ensure the operational information systems security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.

(8) Ensure the establishment, administration, and coordination of security for systems that the DAA's command or organization operates.

(9) Ensure records are maintained for all information system accreditations or certifications under the DAA's purview, to include use of IA tools within the system.

(10) Ensure that an incident-reporting program is established and security incidents or events are reported to affected parties (i.e., interconnected systems), data owners, etc., in accordance with this manual and CJCSI 6510.01C (reference b).

(11) Ensure that the program manager, in conjunction with the IAM and IAO, defines the system security requirements for acquisitions in the SSAA.

(12) Assign written security responsibilities to the individuals reporting directly to the DAA (e.g., IAM or an IAO if an IAM does not exist).

(13) Approve the classification level required for applications implemented in the network environment.

(14) Ensure the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) approves additional security mechanisms necessary to interconnect to external systems (e.g., encryption and guards) and complies with connection procedures established in CJCSI 6211.02 (reference c).

(15) Ensure that criticality and sensitivity levels of each network, site, system, or application are identified in the SSAA. If applicable, ensure conformance with DODD 5200.39 (reference d).

(16) Review the SSAA to ensure each information system supports the security requirements as defined in the network, site, system, or application and network security programs.

(17) Ensure that organizations plan, budget, allocate, and spend resources to achieve and maintain an acceptable level of security and remedy security deficiencies.

(18) Ensure that a security education, training, and awareness program is in place and actively supported.

(19) Ensure counter-intelligence activities are considered during the certification and accreditation process.

(20) Establish working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in a memorandum of agreement (MOA).

(21) Ensure that when classified or sensitive but unclassified (SBU) information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as encryption and protected distribution systems (PDS) (see National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, reference e).

(22) Appoint the IAM in writing to act as the chief technical IA advisor.

3. Information Assurance Manager. The term “information assurance manager (IAM)” is replacing the term “information system security manager (ISSM)” within the Department of Defense. The IAM in many organizations is the IA officer or individual within the IA staff element.

a. The IAM will comply with security requirements of DOD 5200.2R (reference a), and hold USG security clearance and access approvals commensurate with the level of information processed by the information system.

b. The IAM will execute the following responsibilities:

(1) In conjunction with the program manager, maintain for the DAA the SSAA to document site security improvements and progress towards meeting and maintaining accreditation of information systems.

(2) Implement the SSAA and provide security oversight at single or multiple sites or networks as directed by the DAA.

(3) Coordinate security measures including analysis, periodic testing, evaluation, verification, accreditation, and review of information system installation at the appropriate classification level within the command or organization network structure.

(4) Ensure security instructions, guidance, and standing operating procedures (SOPs) are prepared, maintained, and implemented by each site.

(5) Develop and implement an information system security program.

(6) Review and endorse all information system accreditation or certification support documentation packages.

(7) Oversee all IAOs to ensure that they receive proper technical training and information system policies and procedures are followed.

(8) Ensure IAMs, IAOs, and SAs review weekly alerts, bulletins, and advisories that impact security of site information systems to include DOD Computer Emergency Response Teams (CERTs), US Army CERTs (ACERTs), US Air Force CERTs (AFCERTs), US Navy Computer Incident Response Teams (NAVCIRTs), US Marine Corps CERTs (MARCERTs) and information assurance vulnerability alerts (IAVAs).

(9) Develop reporting procedures, and report security violations and incidents to the DAA and local management, as appropriate.

(10) Monitor implementation of security guidance and direct action appropriate to remedy security deficiencies.

(11) Ensure that procedures are developed and implemented in accordance with configuration management (CM) policies and practices for authorizing use of software on information systems. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the IAM or IAO and approved by the DAA prior to changes. Routine system modifications and IAVA implementation may be preauthorized by the DAA within the SSAA.

(12) Serve as member of the CM board or delegate this responsibility to an appropriate IAO.

(13) Ensure users and system support personnel have the required security clearances, authorization, and need to know and are indoctrinated on organization security practices before granting access to the information system.

(14) Ensure audit trails (system logs) are reviewed periodically (daily or weekly) and audit records are archived and maintained for future reference in compliance with local policies.

(15) Ensure data ownership and responsibilities are established for each information system, to include accountability, access, and special handling requirements.

(16) Maintain a repository for all system accreditation or certification documentation and modifications.

(17) Advise the DAA.

(18) Ensure IAO (or network security officer) are appointed for all information systems and networks within the cognizance of the DAA. In the absence of an IAO, the IAM will act in that capacity.

(19) Attend periodic IAM-level information systems security training as required.

(20) Ensure that system users are provided annual information assurance awareness training, and that system administrator, management, and network security personnel are provided appropriate systems security training for their duties.

4. Information Assurance Officer. The term “information assurance officer (IAO)” is replacing the term “information system security officer (ISSO)” within the Department of Defense.

a. The IAO will comply with the requirements of DOD 5200.2-R (reference a) and hold a USG security clearance and access approvals commensurate with the level of information processed by the information system.

b. The IAO will execute the following responsibilities:

(1) Attend required technical (e.g., operating system, networking, or system administration) and security (e.g., security management) training relative to assigned duties.

(2) Ensure the information system is operated, used, maintained, and disposed of in accordance with security policies and practices.

(3) Ensure the network, site, system, or application information system is certified and accredited.

(4) Ensure accreditation and/or certification support documentation package for system(s) for which they are responsible is developed, maintained, and updated as required.

(5) Ensure users and system support personnel have the required security clearances, authorization, and need to know; are indoctrinated; and are familiar with internal security practices before granting access to the information system.

(6) Enforce security policies and safeguards on all personnel having access to the information system for which the IAO is responsible.

(7) Serve as member of the CM board if designated by the IAM.

(8) Initiate protective or corrective measures to maintain security on information systems.

(9) Ensure warning banners are placed on all monitors and appear when a user accesses a system.

(10) Notify the IAM and DAA when changes occur on information system(s) that might affect accreditation and/or certification.

(11) Report security incidents to the IAM and/or DAA in accordance with component guidance, this manual, and CJCSI 6510.01C (reference b).

(12) Report the security status of the accredited environment as required by the DAA, and update the SSAA as the information system is modified or new components are added.

(13) Conduct periodic reviews to ensure compliance with the accreditation and/or certification support documentation package.

(14) Follow procedures developed by the IAM, in accordance with CM policies and practices, for authorizing software use prior to its implementation on an information system. Any changes or modifications to hardware, software, or firmware of an information system must be coordinated with IAM and approved by the DAA prior to the change.

(15) Ensure support to information assurance vulnerability management (IAVM) requirements and ensure security patches are installed, as appropriate.

(16) Ensure users and system administrators of the system(s) or network(s) are provided appropriate annual network security training.

## 5. System Administrators

a. SAs will comply with the security requirements of DOD 5200.R (reference a), and hold a USG security clearance and access approvals commensurate with the level of information processed by the information system.

b. The SA will execute the following responsibilities:

(1) Maintain information system and networks, to include hardware and software.

(2) Monitor information system performance and system recovery processes to ensure security features and procedures are properly restored.

(3) Work closely with the IAO to ensure the information system or network is used and administered securely.

(4) Participate in the incident reporting program and conduct reporting in accordance with this manual.

(5) Provide customer support and ensure that all users have the requisite security clearances, authorization, need to know, and are aware of their security responsibilities before granting access to the information system.

(6) Assist the IAO in ensuring the system is operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the accreditation and certification support documentation package.

(7) Confirm software licenses and documentation are maintained by the configuration management office, and notify the IAM and IAO when changes occur that might affect accreditation and certification.

(8) In coordination with CM office, ensure CM for security-relevant information system software and hardware, to include information system warning banners, is maintained and documented. Apply appropriate security technical implementation guides (STIGs) and periodically re-verify compliance.

(9) Assist IAM and IAO in development and maintenance of accreditation and certification support documentation package.

(10) Establish audit trails (system logs) and conduct reviews periodically (weekly or daily), and ensure audit records are archived for future reference as directed by the IAO and IAM.

(11) Provide backup of system operations.

(12) Conduct periodic reviews to ensure compliance with the accreditation and certification support documentation package.

(13) Respond to IAVAs, information assurance vulnerability bulletins (IAVBs), and other vulnerability notifications by obtaining and installing system patches, making procedural changes, and reporting IAVA compliance to the appropriate authority (see Appendix A to Enclosure B, "Information Assurance Vulnerability Management Program").



(14) In coordination with CM office, maintain and document the CM of the information system to include software, hardware, and warning banners. Assist the IAO in maintaining configuration control of the systems and applications software.

(15) Advise the IAO of security anomalies or integrity loopholes.

(16) In coordination with the IAO, administer user identification and authentication mechanism(s) of the information system or network.

(17) Attend required technical (e.g., operating system, networking, or system administration) and security (e.g., security management) training relative to assigned duties.

6. Program Managers, Certification Authorities, and User Representatives.  
Under DITSCAP, the program manager, certification authority, and user representative have certain responsibilities (DODI 5200.40, reference f).

a. Program Manager (PM) Responsibilities

(1) Define system schedule and budget.

(2) Define and/or validate system performance, availability, and functionality requirements.

(3) Support DITSCAP tailoring and level-of-effort determination.

(4) Draft or participate in drafting the SSAA. Review and approve the SSAA and revisions in coordination with the DAA, CA, and user representative.

(5) Develop system or system modifications.

(6) Support certification actions.

(7) Review certification results.

(8) Revise the system, as applicable.

(9) Test the integrated system.

(10) Operate the system as described in the SSAA.

(11) Maintain an acceptable level of residual risk.

(12) Submit proposed changes to the user representative, the IAO, the DAA, and the CA, as applicable.

(13) Support compliance validation.

(14) Ensure system is fielded with security plans and associated documentation.

b. CA Responsibilities

(1) Draft or participate in drafting the SSAA. Review and approve the SSAA and revisions in coordination with the DAA, PM, and user representative.

(2) Perform certification actions.

(3) Evaluate developing system.

(4) Assess vulnerabilities and residual risk.

(5) Report results to the PM, the DAA, and the user representative, and make recommendation on accreditation or operations limitations to the DAA.

(6) Prepare the accreditation package.

c. User Representative Responsibilities

(1) Validate and/or define system performance, availability, and functionality requirements.

(2) Support DITSCAP tailoring and level-of-effort determination.

(3) Reach agreement on the SSAA. Review and approve SSAA and revisions in coordination with the DAA, PM, and CA

(4) Support certification actions.

(5) Review certification results.

(6) Oversee system operation as described in the SSAA.

(7) Maintain an acceptable level of residual risk.

(8) Continuously review threat, system vulnerabilities, and residual risk.

(9) Review and approve proposed changes.

(10) Submit significant changes to the DAA and the CA.

(11) Perform compliance validation actions.

#### 7. Individuals and Information System Users

a. DOD individuals have a personal responsibility to protect DOD information processed on information systems.

b. All DOD military, civilians, and contractors will:

(1) In-process and out-process as directed by local policies.

(2) Receive documented training prior to network access and receive training annually. (See Appendix B of Enclosure A, "Training, Education, and Certification.")

(3) Acknowledge consent to monitoring DOD networks. (See paragraph 8 this appendix and Appendix C, Enclosure C, "Electronic Notice and Consent Banner.")

(4) Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.

(5) Use DOD information systems only for official use and authorized purposes in accordance with DODI O-8530.2 (reference g).

(6) Only access data or use operating systems (OSs) or programs as authorized.

(7) Use USG-acquired hardware and software to the maximum extent possible.

(8) Use personally owned hardware, software, shareware, or public domain software only with the expressed permission or approval of the DAA.

(9) Protect controlled unclassified information and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.

(10) Properly mark and safeguard SBU information so that only authorized persons have access, it is used only for its intended purpose, and it retains content integrity.

(11) Mark all information created, copied, stored, or disseminated on DOD automation networks whether in the form of messages, electronic mail, word processing documents, spreadsheets, databases, graphical presentations, or art with the appropriate classification level in accordance with Executive Order (EO) 12958 (reference h) and DOD 5200.1-R (reference i). Unclassified information should be marked as such when located on classified systems. The classification of information contained in nonhuman readable formats at protocols will be described in the system documentation.

(12) Administer and protect passwords for systems requiring logon authentication. The minimum requirement is a password consisting of a mix of at least eight characters using three of four character sets (uppercase letters, lowercase letters, numbers, and special characters). Do not use user identification (ID), common names, birthdays, phone numbers, consecutive numbers or letters, alphanumeric sequential combinations, or dictionary words. Users will be informed that SAs will employ password tools to identify weak or non-compliant passwords. Note: Eight characters are the DOD minimum requirement. If technically feasible, 12 to 16 characters using a mix of all four-character sets is recommended.

(13) Safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.

(14) Screen-lock the workstation when leaving the work area, and use password-protected automatic screen savers where available. Log off or power down the workstation at the end of each working day or when leaving the work area for an extended period as defined by local security guidance.

(15) Allow no maintenance to be performed on any workstation without authorization.

(16) Virus-check all information, programs, and other files prior to uploading onto any DOD information system.

(17) Do not upload executable files (e.g., .exe, .com, .vbs, or .bat) onto DOD information systems without the approval of the DAA.

(18) Do not write malicious code. Note: This does not include official red teaming and other authorized IA testing.

(19) Report all security incidents immediately in accordance with local procedures and Appendix B to Enclosure B, "Incident and Vulnerability Reporting," of this manual.

## 8. Network Suspensions

a. Combatant commands, Services, and/or agencies (C/S/As) will all suspend network access for, at a minimum, the following types of actions:

(1) Actions that knowingly threaten, damage, or harm DOD information systems, networks, or communications security (e.g., hacking or inserting malicious code or viruses).

(2) When an individual has a security clearance and that clearance is suspended, denied, or revoked; or a person in the process of obtaining a clearance is denied an interim clearance.

(3) Unauthorized use of the same.

b. Suspension is not, in and of itself, a punitive action. C/S/As will develop their own policies governing network suspensions and reinstatements. Suspensions related to clearances must follow the guidelines of DOD 5200.2-R (reference a).

9. User Agreement. Each C/S/A must ensure new users are briefed on their individual information and information system security responsibilities, consent to monitoring, and have signed a user agreement prior to system access.

a. User agreements will be maintained at a level determined by the C/S/A. The content of organization user agreements should be reviewed periodically to meet current requirements and regulations.

b. The following is provided as an **example user agreement** that can be modified for local requirements and regulations.

This memo details some of the duties and requirements established by existing law, executive orders, regulations, and instructions for the use of (*Insert your organization*) systems.

1. (*Insert organization's classified information network (OCIN)*) and (*insert organization's unclassified network (OUNET)*) users have the responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. *OCIN* and *OUNET* are for official use and authorized purposes in accordance with DOD 5500.7-R, "Joint Ethics Regulation" (reference j). Information on both systems is subject to monitoring and security testing.

2. *OCIN* is the primary classified automated administration tool for the (*insert your organization*). *OCIN* is a US-only system and approved to process TOP SECRET collateral information as well as NATO SECRET and NATO ATOMAL. *OCIN* is not authorized to process sensitive compartmented information, SIOP, NATO COSMIC, or information requiring special access programs.

a. *OCIN* provides communication to external DOD or any USG organizations using the SECRET Internet Protocol Router Network (SIPRNET). This is done via electronic mail and network protocols from *OCIN*.

b. The SIPRNET is authorized for SECRET or lower-level processing in accordance with (*Insert local regulation dealing with automated information system security management program.*)

c. The classification boundary between *OCIN* (TOP SECRET) and SIPRNET (SECRET) requires vigilance and attention by all users. SIPRNET is also a US-only system and not accredited for transmission of any NATO material.

d. The ultimate responsibility for insuring the protection of TOP SECRET information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation.

3. *OUNET* is the primary unclassified automated administration tool for the (*Insert your organization*). *OUNET* is a US-only system.

a. *OUNET* provides unclassified communication to external DOD and other USG organizations using the Non-classified Internet Protocol Router Network (NIPRNET). This is done via electronic mail and network protocols from *OUNET*.

b. OUNET is approved to process UNCLASSIFIED, nonsensitive information in accordance with (Insert local regulation dealing with automated information system security management program).

c. The NIPRNET and the Internet, as viewed by the (Insert your organization) are synonymous. Minimal security exists on this system. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

4. As an OCIN and/or OUNET system user, the following security rules and requirements apply:

a. Personnel are not permitted access to OCIN and OUNET unless in complete compliance with the (Insert your organization) personnel security requirement for operating in a TOP SECRET system high environment.

b. The (Insert your organization) training program is required for all personnel before receiving system access. The security awareness- training module, as a minimum, is required for contract personnel.

c. Passwords must be safeguarded. Personal password sharing and embedded passwords is prohibited.

d. Secure passwords will consist of at least eight (or insert local requirement (e.g., 12 characters)) characters and random combinations of uppercase and lowercase letters, numbers, and special characters. Do not use your user ID, common names, birthdays, phone numbers, or dictionary words.

e. Only USG-acquired hardware and software are authorized. Use of any personally owned hardware, software, shareware, or public domain software without the expressed permission or approval of the OCIN/ OUNET DAA is prohibited.

f. Virus-checking is mandatory prior to uploading information onto any (Insert your organization) system via SIPRNET, NIPRNET, diskettes, or compact disks.

g. Users will not attempt to access or process data or use operating systems or programs, except as specifically authorized. Users will not upload .exe, .com, .vbs or .bat files onto either system without DAA permission. Users will write no malicious code.

h. Users will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated on office automation networks (i.e., printed output, magnetic tapes, floppy disks, and downloaded hard-disk files) whether in the form of messages, electronic mail, word-processing documents, spreadsheets, databases, graphical presentations, or are IAW EO 12958, "Classified National Security Information," (reference h) and DOD 5200.1-R, "Information System Security Program" (reference i).

i. No maintenance will be performed on any workstation without authorization from the (*insert your organization*) system administrator.

j. Log-off or screen-lock the workstation when leaving the area. Log-off the workstation at the end of each working day.

k. Users can notify (*insert your organization*) system administrator and/or (*insert your organization*) information systems security officer with any questions regarding policy, responsibilities, and duties. Do not hesitate. Report all security incidents immediately.

l. Report information system or network problems to the SA.

m. The system(s) is(are) subject to monitoring for management of the system, protection against unauthorized access, and verification of security procedures.

n. Authority for soliciting a social security number (SSN) is EO 939. The information below may be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting a violation of the law. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access (*insert your organization*) systems.

5. I have read the above requirements regarding use of (*insert your organization*) access systems. I understand my responsibilities regarding these systems and the information contained in them.

\_\_\_\_\_  
Directorate/Division/Branch

\_\_\_\_\_  
Date

\_\_\_\_\_  
Last Name, First, MI    Rank/Grade

\_\_\_\_\_  
SSN

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Phone Number



## APPENDIX B TO ENCLOSURE A

### TRAINING, EDUCATION, AND CERTIFICATION

1. General. Information technology has enabled USG to transmit, communicate, collect, process, and store unprecedented amounts of information. The importance of information systems used by the federal government has focused attention on the need to ensure that these assets and the information they process are protected from actions jeopardizing the ability to function effectively. Responsibility for securing this information and its systems lies with the head of the owning federal department or agency. The trained and aware worker is the first and most vital line of defense protecting DOD information and information systems.

#### 2. DOD Training and Certification Objectives

a. Enhance awareness of all persons within the Department of Defense for the need to ensure protection of information in systems, as well as systems resources and capabilities.

b. Promote protection of information systems at the national level by promoting uniform and consistent understanding of the principles and concepts of information and information systems protection.

c. Enhance the knowledge and skills needed to mitigate risk by eliminating vulnerabilities.

d. Ensure varying competence levels among DOD system users, administrators, and network operations personnel (including military, government civilian, and contractor personnel) appropriate to their level of responsibilities.

e. Standardize skill sets to support rapid contingency expansions.

f. Provide warfighters with technically competent workforce, both in information technology (IT) functional responsibilities and in information security, operating at skill levels commensurate with their duties and responsibilities.

g. Provide a formal process achieved through a combination of resident courses, supervised hands-on, on-the-job training, local contracted courses, and applicable computer-based training modules.

- h. Provide annual refresher training to improve and maintain system skills.

3. IA and Information Security. IA and information security (INFOSEC) education, training, and awareness activities are required for all employees annually, to the degree necessary on related job functions. Such a comprehensive effort must meet the varying levels of employee knowledge, experience, and responsibilities, and specific needs of C/S/A. Certain themes that need to be conveyed:

- a. Organizations critically rely on information and information systems resources.

- b. The organization, through its management, commits to protect information and information system resources.

- c. Threats, vulnerabilities, operational impacts, and related risks associated with the organization's information systems exist.

- d. Consequences exist for inadequate protection of the organization's information systems resources.

- e. The employee is the essential element of a successful protection program.

4. Training, Education, and Certification

- a. Security education, training, and awareness are essential to a successful IA program. Employees who are informed of applicable organizational policies and procedures are expected to act effectively to ensure the security of system resources. General users require different training than those employees with specialized responsibilities.

- b. Training product information and available products can be found at <http://iase.disa.mil/eta/index.html>.

- c. Making information systems users aware of their security responsibilities and teaching them correct practices helps users change their behavior and support individual accountability -- one of the most important ways to improve computer security. Without knowing the necessary security measures (and how to use them), users cannot be truly accountable for their actions.

d. Initial IA training standards to support defense-in-depth were established by the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence (ASD(C3I)) Joint Memorandum, "Information Assurance (IA) Training and Certification," 29 June 1998 (reference k). The memorandum addresses requirements for user and systems administrator certification.

e. The DOD requirement to develop and implement INFOSEC education, training, and awareness programs for national security systems was established by National Security Telecommunications and Information Systems Security Directive (NSTISSD) 500 (reference l). This policy is applicable to USG departments and agencies, their employees, and contractors. DOD components will develop, implement, and evaluate INFOSEC education, training, and awareness programs in accordance with National Security Agency (NSA) and other applicable guidelines. These programs must:

(1) Use applicable information copies of INFOSEC education, training, and awareness materials available from the NSA and the Defense Information Systems Agency (DISA) consistent with applicable laws, security requirements, and policies.

(2) Contain three types of activities:

(a) Initial orientation,

(b) More advanced awareness, education, and training commensurate with specific duties and responsibilities.

(c) Reinforcement activities.

(3) Be conducted by individuals knowledgeable of INFOSEC principles, concepts, and application.

5. Minimum User IA Training and Awareness. All users will train annually. C/S/As will conduct, document, and maintain status of training for each user. System access will not be authorized without appropriate documented training. Users of classified networks will not receive network access without IA training. At a minimum, users will train annually on the following:

a. The need for INFOSEC and IA, to include public law, DOD policy, common sense, and the threat (see below).

b. Threats to DOD systems:

(1) External threats, such as script kiddies, crackers, hackers, protesters, zombie scripts (Code Red), agents employed by terrorist groups or foreign countries, and acts of nature.

(2) Internal threats, threat agents such as malicious or incompetent insiders, insiders employed by terrorist groups or foreign countries, disgruntled employees or Service members, hackers, crackers, and self-inflicted intentional or unintentional damage.

c. DOD risk from aggregation of unclassified information.

d. Principle of shared risk in networked systems (i.e., how a risk assumed by one is imposed on the entire network).

e. Risks associated with remote access; e.g., working from home, during deployment, or on temporary duty.

f. Privacy issues, including vulnerability of administrative, financial planning, travel-related, payroll, medical, and personnel records during transmission and similar vulnerabilities in sensitive E-mail.

g. Malicious code; e.g., logic bomb, Trojan horse, malicious mobile code, viruses, and worms; how they attack; and how they damage an information system.

h. Impact of distributed denial of service (DOS) attacks.

i. Prevention of self-inflicted damage.

j. Scope of embedded software and hardware vulnerabilities and how the Department of Defense corrects them (e.g., IAVM process).

k. Unauthorized activity on local systems and how to report unauthorized or suspicious activity.

l. Basic differences between NIPRNET and SIPRNET and why they are protected differently.

m. Information operations condition (INFOCON) requirements and definition.

n. Local IA chain-of-command roles and responsibilities for the IAO, IAM, systems administrators, and help desk, if applicable.

## 6. SA Certification

a. The certification program for SAs should include the following subject areas: configuration control; installation; operations and maintenance; user account management; system selection; access control; response, recovery, and/or reconstitution; incident response; operations monitoring and analysis; and countermeasures.

b. All SAs, including part-time or collateral-duty SAs, will be certified and cleared to the level of information classification of a given information system. Training need not award military specialty or training codes (i.e., military occupational specialty, naval educational code, and/or Air Force Specialty Code), but must be sufficient to meet minimum certification standards outlined below. Part-time SAs are commonly found in specialty communities (e.g., logistics, medical, or tactical systems only used on deployment). Contractor SAs will also meet certification and information clearance standards.

c. C/S/As will conduct certification of their SAs.

d. C/S/As will document and maintain certification and information clearance status of SAs.

e. Certification standards will apply equally to uniformed Service members, DOD civilians, and contract personnel. Contract language will include the certification level appropriate for the requirement, and negotiate civilian equivalencies as necessary.

f. Level 1 SA certification of SAs is mandatory prior to issuing unsupervised root access. DAAs may waive this requirement under severe operational or personnel constraints. DAAs will document the waiver using a memorandum for record stating the reason for the waiver and the plan to rectify the constraint. Waivers must be time limited and include an expiration date.

g. SAs must certify and renew certifications annually to retain system access. Persons who are not certified or who fail certification tests will not be permitted root, administrative network, and/or system access. C/S/As will develop programs to address remedial training and conditions for workers to return to certified status.

## 7. SA Certification Requirements

a. USD(P&R) and ASD(C3I) memorandum (reference k) and NSTISSD 501 (reference m) establish the requirement for USG departments and agencies to implement training programs for IA professionals. NSTISSI 4013 (reference n) provides national training standards for SAs.

b. The following paragraphs provide certification requirements for DOD systems administrators. They are designed as high-level task sets from which C/S/As will develop their own tailored training task lists.

c. Because extensive recommendations already exist on technical tasks, the list is oriented to operational military IA tasks. Those tasks applying exclusively to military operations are marked with an asterisk (\*); agencies for whom they do not apply will not be responsible to train those tasks.

d. All skill levels require security background investigations in accordance with DOD 5200.2-R (reference a).

## 8. Skill Level 1 SA

a. Novice or Beginner. Skill level 1 administrators generally have minimal experience (e.g., less than 3 years) in the job. Skill level 1 SAs are generally in the grades of E-3 to E-5 or civilian equivalent and have lesser responsibility (e.g., small localized local area network (LAN) with few users and no additional servers other than the domain controller). (Note: A operational information systems security compact disk set is available from DISA.)

b. Skill Level 1 Training Requirements (see Table A-B-1)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Formal training on the OS and command language or network protocols/operating parameters (network administration).		Understand computer operating system fundamentals.		
Know rudimentary system/network administrator tasks relevant to the OS or network device.		Understand and perform basic OS tasks.	2.2C	
Know OS, command language, and/or network protocols.	Manage system hardware and software.		2.2C	1 b 2 c
	Manage accounts. Maintain data store.			2 d 5 c
	Provide communication connectivity and configure network protocols.	Install OSs, applications and peripherals; conduct testing and safeguards.	3.3D 3.3E	1 b 5 b
Know normal operating parameters of relevant systems and applications.			2.2C 3.3C	1 a 1 b 2 c

Table A-B-1. Skill Level 1 Requirements

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know basic system /configuration troubleshooting.	Troubleshoot problems.	Recognize abnormal operations. Recognize potential threats.	3.1C 3.3C	1 b
	Install and verify software patches.	Understand and perform basic system configuration and troubleshooting.	3.5D	1 b
		Conduct informal, on-the-spot user assistance and training.		1 b 1 c
General knowledge of security features of operating systems and applications.		Understand network security basics.		1 a
		Understand the purpose of security devices (e.g., firewalls, host/network based intrusion detection systems, virtual private networks, and malicious code scanners.	2.2D 3.1C 3.2B	1 a 2 d 4 b 5 b

Table A-B-1. Skill Level 1 Requirements (cont'd)



<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Understand appropriate network and computer monitoring procedures.	2.2D 3.1C 3.2B	2 b
		Understand the available mechanisms for detecting malicious code.	2.2D 3.1C 3.2B	5 b
		Understand the definition and purpose of cryptography.	2.2D 3.2B	
	Manage system security parameters	Able to configure system/network and application security parameters as required.	3.4D 3.5D	5 b 5 c 6 b
Formal training on IA awareness and common system/network vulnerabilities.		Understand the evolution and principles of INFOSEC.		1 a
		Understand and identify threats to information and information infrastructure.	3.1C	1 e

Table A-B-1. Skill Level 1 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Understand common vulnerabilities within an information infrastructure.	3.4D 3.5D	1 c
		Understand the definition and characteristics of malicious code.	3.4D 3.5D	1 c
	Ensure security. Protect, detect, and react against system incursions.	Understand the principles of access level privileges (rings of protection/least privilege concept).		2 b 6 b
		Assist IAO in access control security (passwords, auditing and alarming, etc.).	2.1B	4 b 4 c
Know local IAVA procedures.		Understand and react to vulnerability alerts (e.g., IAVAs).		1 a 1 b
Know local procedures for incident reporting and how to contact security assistance.		Receive and initiate incident reports.	1D	1 b
Basic knowledge of command/organization's mission.				1 a

Table A-B-1. Skill Level 1 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Basic knowledge of command/organization networks and systems.		Understand network topologies.	2.2C	1 a
		Understand internet working fundamentals.	2.2C	1 b
		Understand the principles of risk management and risk mitigation.	2.2C	1 e
Know priorities for command/organization networks and systems restoration		Understand disaster recovery and continuity of operations concepts.	2.2D	5 a
		Understand and perform system backup operations.	3.5D	6 a
		Install emergency workarounds, as directed.	3.5D	5 b 5 c
Know about destruction plans and likely scenarios that trigger their execution.	Destruction techniques.	Assist with emergency destruction planning and execution.	3.5D	5 a 6 c

Table A-B-1. Skill Level 1 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know basic differences between deployed (tactical) and garrison operating environments.* (agencies may want to focus on IA planning for rapid wartime/contingency expansions.	LAN installation/repair. Network/system installation and repair. User assistance.	Able to operate in garrison and deployed environments, as required.*	2.1B 2.1C	
Know how to safeguard classified and sensitive data, both physical and electronic.	Maintain expertise.	Understand handling security procedures for classified/sensitive data.	1D 1E	1 b
		Understand physical security principals.		1 a
		Enforce physical and cyber-based security procedures.	3.5D	1 b

Table A-B-1. Skill Level 1 Requirements (cont'd)

9. Skill Level 2 SA

a. Skill level 2 SAs are more experienced (3 to 5 years). Skill level 2 SAs are generally in grades E-5 to E-7 or the civilian equivalent and have greater responsibility (e.g., large network with multiple domains, several types of servers, and a larger user population). 50 percent or more of the SAs should be skill level 2 in organizations operating large mission-critical networks with multiple domains, several types of servers, and large user populations.

b. Skill level 2 SAs must demonstrate mastery of all skill level 1 tasks. Mastery should be assessed on the job and through a combination of hands-on and written testing. In addition to skill level 1 tasks, these SAs should acquire

the following sets of knowledge, skills, and abilities. Specialization (network administration, security administration, etc.) on particular aspects of computers and networks may occur at higher skill levels.

c. Skill Level 2 Certification Requirements (see Table A-B-2)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Formal training in networking, programming language concepts, and algorithms.		Able to program in a command language.		
Formal training in vulnerability scanners, host based intrusion detection, and other security tools.		Install and configure firewalls and proxy servers.	3.4D 3.5D	2 b 4 c 5 b
		Install and configure host and network-based intrusion detection systems.	3.4D 3.5D	6 b
		Understand and implement access control mechanisms.	2.2D 3.4D	2 a 2 b 2 c
		Identify and configure auditing and logging capabilities.	3.4D 3.5D	2 d

Table A-B-2. Skill Level 2 Requirements

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Understand and configure public key based cryptographic mechanisms.	3.5A	
		Understand application level security architecture models (e.g., JAVA, ActiveX, etc.).	3.5A	
		Provide assistance in testing security mechanisms.	3.1E 3.1F 3.2D 3.3D	
Know networking algorithms and program language concepts. Know telecommunications networking, key management, network design, configuration, and interconnections.	Provide network/system connectivity.		3.5D	1 a 1 b 5 c
Know how to administer the relevant OSs and applications.			3.5D	1 a 1 b 2 c 5 c
	Manage system hardware and software.	Configure and implement network based protocols.	3.4D 3.5D	2 c

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Configure and manage file, print, and web server hardware and software.	3.4D 3.5D	5 c
		Configure and manage client workstation hardware and software.	3.4D 3.5D	5 c
	Maintain data store. Ensure the validity and reliability of data files.		3.5D	2 d 5 c
	Interact with developers, operations centers, and support personnel to maintain reliable operations. Continually monitor health of system.		2.2C 3.1F 3.2D 3.3D	5 c
	Solve complex problems.	Independently solve complex network and security problems.	2.2E	5 b 6 b
		Explain solutions for complex problems to users and other SAs.	2.2E 3.4E 3.5E	1 c
		Train skill level 1 SAs.	3.5A	1 c

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
	Interact with others.	Strong communications and customer relations skills.		
	Manage accounts.	Conduct account management.	3.5D	2 a 2 d
		Understand the mechanisms for maintaining user accountability.	3.4C	2 c
Know how to implement firewall management, intrusion detection, and available security tools.	Ensure security. Protect detect, react against system incursions.		3.5E 3.5F	1 b 2 b 5 b 6 b
	Plan and implement defense-in-depth for networks, enclaves, computing environments and infrastructure.	With IAO, plan most effective use of security tools.	2.1B 2.1D	4 c 6 b
		Analyze threats. Identify differences between technical problems and security incursions.	2.1B 2.1D 2.2E	3 b 5 c
		Scope, plan and implement countermeasures.	2.1E 3.4D	1 d 2 b 3 b 5 b 6 b

Table A-B-2. Skill Level 2 Requirements (cont'd)



<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know all interactions within domain. Know how to identify abnormal operations.		Monitor network resource utilization.	3.5F	5 c 6 c
		Implement complex operating system changes.	3.4D 3.5D	5 c 6 c
		Monitor and ensure systems are hardened against security vulnerabilities and software operates properly.	3.5F	2 b 5 c
		Establish and monitor internal domains and security enclaves.	3.4F 3.5F	1 e 5 c
		Monitor and balance network/system load. Detect and interpret abnormalities.	3.4F 3.5F	5 c 6 c
		Systematic and continuous inspections IAW technical and security standards.	3.3D	3 a 4 c
	Perform software and hardware troubleshooting.	Complex troubleshooting across networks and systems.	3.5D	6 b

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Configure, manage, and troubleshoot network components.	3.4D 3.5D	6 b
Comprehensive knowledge of command/organization's network and primary external and internal connectivity.	Maintain network/system connectivity.	Be familiar with legal and ethical issues associated with the use and management.	1A 1F	1 a 1 d
Know command/agency mission and priorities. Know which systems/networks are critical, essential, and support.			1A 2.1D 2.1E	1 a 3 a
Know physical and software interfaces for priority systems. Understand alternative/backup systems available for continuity of operations.		Plan, supervise, implement, and inspect emergency work-around and large-scale system restoration.	3.5D	5 a 6 a
		Plan, supervise, implement, and inspect rapid assimilation of surge (crisis) networks.	3.5D	5 c 6 c

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Protect/recover information from loss or damage. Conduct emergency restoration planning and operations.	3.5D	5 c 6 a
Know infrastructure's critical nodes and understand effects of infrastructure failures.		Predict crisis/attack vulnerabilities and losses, to include impact of failed infrastructure and physical destruction of networks/equipment.	3.5D	5 a 6 a 6 b
Know about destruction plans and techniques and when to execute.	Physical destruction techniques.	Plan and implement emergency destruction.	3.4D 3.5D	6 c
Know how to prepare for operations in varied environments (garrison, deployed, etc.), as required.*	Requisition of equipment for varied operating environments, as required.	Operate in varied environments.	3.5D	5 b 5 c 6 c
		Operate during electronic/physical attack.	3.5D	5 b 5 c 6 b 6 c

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know local and DOD security policy and standards.	Implement security requirements.	Understand the DITSCAP.	1A 3.2D 3.4E 3.5E	1 a
		Interpret requirements and implement appropriate security features/policy.	2.1B 2.1D 3.1C	1 a 1 b
		Provide assistance in host network accreditation.	2.1B 2.1E 3.1C 3.4E 3.5E	1 a 1 b
Know physical and electronic protection requirements for sensitive and classified data.		Enforce security policy and procedures. Recognize, analyze and correct deficiencies.	1D	1 a 3 a
		Scope, plan and implement countermeasures from technical vulnerabilities including emerging deficiencies and vulnerabilities.	2.2D 3.4D 3.5D	3 b 4 b 5 a 5 b

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know local procedures for incident reporting and IAVAs.		Understand security incident reporting procedures.	1A	1 a 5 a
		Implement incident response and reporting procedures.	1D 1F 3.4D	5 b 5 c
		Provide assistance in incident handling.	1D 3.5D	5 c
		Understand and implement vulnerability reporting procedures.	1D 3.4D	5 c
Know DOD and local rules of engagement for responding to network attacks; understand legal implications or response.	Preserve evidence of attack, tampering.	Respond to attack IAW rules of engagement and applicable law.	1A 1D 3.5D	1 a
Know appropriate web security measures.	Maintain expertise.		3.4C	1 d 1 e

Table A-B-2. Skill Level 2 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Know OPSEC and privacy issues regarding the storage, release, and display of personal data. Understand OPSEC issues on posting material to websites.		Able to determine appropriate material for web release.	1A	1 a 2 a
Know associated vulnerabilities of command's/ organizations interconnected and interdependent systems.	Maintain expertise. Maintain current knowledge on network vulnerabilities and solutions.	Understand the nature of network and information systems attacks.	2.2C	1 c 1 e
		Understand the policies that assist in preventing, detecting, and containing threats.	1A	1 a
		Understand the security implications associated with the use of mobile code and scripts.	2.2D	2 a

Table A-B-2. Skill Level 2 Requirements (cont'd)

10. Skill Level 3 SA

a. Skill level 3 SAs are highly experienced (more than 5 years). Skill level 3 SAs are generally in the higher military grades (officers, warrant officers, senior enlisted) or civilian equivalent and are responsible for managing resources, policy, and/or supervising other SAs. SAs at level 3 may also include specialized civilians with advanced skills.

b. Skill level 3 SAs must demonstrate mastery of skill levels 1 and 2 tasks (see Table A-B-3).

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800- 16</b>	<b>NSTISSI # 4013</b>
Knowledge of OS design, data/algorithm structure, machine architecture, networking, programming language, and concepts. Knows network design, key management, configuration, and interconnections.		Plan and coordinate system modifications (e.g., network installation, software reconfigurations, etc.).	2.1B 3.1F 3.2D	5 c 6 c
		Plan account management strategy.	2.1B	2 a
Knows applicable programming language(s) and security vulnerabilities of those languages.	Expert management of system hard/software and data storage. Expert management of application software.	Define hardware/software requirements.	2.1B 3.2B 3.3E	1 a 2 a
		Plan data storage layout.	2.1B	3 a

Table A-B-3. Skill Level 3 Requirements

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Understands strategic view of the networks operation and mission, as well as internal and external interactions.		Understand the organizational structure for defensive information operations.	1A	1 a 1 d 1 e 3 a
		Tune the performance of existing domains; monitor for attacks and problems.	3.4D 3.5D	5 b 5 c 6 b 6 c
Strong interpersonal, organizational, and communications skills.	Work independently or lead teams to quickly and completely solve problems.	Solve complex problems involving external and internal assets/issues. Articulate network and command/agency requirements.	2.1B 2.1D 3.4D 3.5D	1 a 1 b
		Lead teams to tackle complex security problems.	3.5D	3 a
In depth knowledge of local and DOD security and IA policies.		Assist in development of system security policy.	1A	1 a
		Understand the details of communications security (COMSEC) monitoring policies.	1A	1 a

Table A-B-3. Skill Level 3 Requirements (cont'd)



<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Develop local system administrator sustainment training plan.	3.5A	1 c
		Develop and implement vulnerability assessment procedures.	1D	1 b 3 b 5 b
Current knowledge of security devices and procedures.	Ensure security. Protect, detect, and react against systems incursions.	Plan and design the security architecture.	2.1B 2.1D 3.1C, E, F 3.2E 3.3E	1 b
		Be familiar with emerging threat tools and techniques.	3.2D	4 c
		Advise commander on IA and INFOSEC /privacy issues for data storing and posting. Assist in the establishment of end user security guidelines.	1D 1E	1 d 2 a 3 a 3 b
		Set and interpret standards, security procedures and safeguards. Establish audit and logging guidelines.	2.1B 2.1D	3 a 4 b

Table A-B-3. Skill Level 3 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
		Enforce security procedures	1D 3.4D 3.5D	3 a
		Advise public affairs and local webmasters on web security issues	1D	3 b
In depth knowledge on limits of response and DOD/local rules of engagement		Understand legal and ethical issues associated with the use and management of IT resources. Analyze IT security laws, vulnerabilities, and recognize the legal ramifications of attack responses and interpret appropriate rules of engagement.	1A 1D	1 a
Know how to design and implement defense-in-depth.	Assess, manage, and plan implementation of countermeasures for technical vulnerabilities.	Develop technical plans for implementing network and host based security countermeasures (e.g., cryptography, intrusion detection, etc.).	2.1B 3.1A 3.1C 3.2D	1 a 1 b 1 e

Table A-B-3. Skill Level 3 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Understand principles of managing risk.		Understand and apply risk management principles. Able to weigh benefits versus risks. Can articulate it.	2.2C 2.2D 2.2E	1 e 5 c
Know user requirements and network/system capabilities.		Balance user requirements (mission) against network/system capabilities.	1F 2.2D 2.2E	1 5
Understand operational priorities and which systems and infrastructures support them.		Plan backup and restoration procedures.	3.5C	5 a 6
		Understand and develop strategies for overcoming data integrity problems caused by hardware, software, and other unintended modifications.	3.1C 3.2D 3.5C	
Know technical and operational implications of outages and interruptions.			3.5A	3 b

Table A-B-3. Skill Level 3 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
Understand infrastructure vulnerabilities and their potential to affect the network.		Conduct systematic analysis of attack implications. Interpret impact of outages and rapidly issue alternative plans.	2.2C 2.2D	5 6
Know potential attack threats and most likely damage.		Predict crisis/attack losses and network vulnerabilities across scope of conflict.	3.5D	5 6 3 1 e
		Manage, predict, and rapidly assimilate surge (crisis) users.	3.5D	5 6
		Integrate tactical and strategic networks/systems and security issues.*	3.5D	6 a 6 c
		Plan and provide materiel for transition to varied operating environments (garrison to deployed, etc.).*	2.1B 2.1D	5 6

Table A-B-3. Skill Level 3 Requirements (cont'd)

<b>Knowledge</b>	<b>Skill</b>	<b>Ability</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4013</b>
	Destruction techniques.	Produce standard and emergency restoration orders, destruction plans, and continuity or operations plans.	3.5C	5 6
Detailed knowledge on organization's budget cycle.		Able to create and manage a budget.	2.1A	
Knows how to make proposals and presentations, write plans and orders.				3 a 3 b
	Training techniques.	Able to train skill levels 1 and 2 SAs. Able to assess value of training.	3.5A	1 c

Table A-B-3. Skill Level 3 Requirements (cont'd)

11. Additional IA Professionals

a. Individuals carrying out duties in computer and/or network crime, threat and vulnerability assessments, CERT and computer incident response team (CIRT) positions, and C/S/A information system security staff positions will be, at a minimum, certified as skill level 1 SAs for IA and be provided training in one or more of the following areas:

(1) Computer and Network Crime. The training program for this critical function should include:

- (a) Knowledge of forensic analysis and technical expertise in computer and network crime.
- (b) Knowledge of computer crime laws and regulations.

(2) Threat and Vulnerability Assessments for Information Systems. The training program for this critical function should include the following subject areas:

- (a) Assessment policy and procedures.
- (b) Red Team operations and network-penetration testing.
- (c) Information system threat analysis.

(3) CERT and CIRT. The training program for these critical functions should include the following subject areas:

- (a) Collecting, reporting, and managing technical vulnerability information.
- (b) Collecting, reporting, and managing incident reports.
- (c) Providing victim site technical expertise to mitigate and reconstitute following an event or incident.
- (d) Disseminating vulnerability information with mitigation solutions.
- (e) Disseminating threat information.
- (f) Coordinating with other CERTs and CIRTs.
- (g) Coordinating with law enforcement agencies.

(4) Web Site Security. The training program for this critical function should include the following subject areas:

- (a) Information management.
- (b) Information system administration.
- (c) Information system security.
- (d) Critical indicator information and OPSEC training.

(5) Other Specializations. Other areas of specialization can include Microsoft Windows security, universal interactive executive (UNIX) security,

router security, mobile device security, firewall security, remote access security, and wireless security.

b. Table A-B-4 provides National Institute of Standards and Technology (NIST) Standard #800-16 (reference o) and NSTISSI No. 4014 (reference p) applicable national training standards for IAO responsibilities in Appendix A.

<b>IAO Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4014</b>
1. Attend required technical (e.g., operating system, networking, or system administration) and security (e.g., security management) training relative to assigned duties		
2. Ensure the information system is operated, used, maintained, and disposed of in accordance with security policies and practices.	1D 2.1D 2.2D 3.2D 3.3D 3.4D 3.5D 3.6D	1 b 2 4 a, 4 c, 4 e 7 b
3. Ensure the network, site, system, or application information system is certified and accredited.	3.2E 3.3D 3.3E 3.4E 3.5E	1 b 3
4. Ensure accreditation/certification support documentation package for system(s) for which they are responsible is developed, maintained, and updated as required.	2.1A 3.3D 3.4E 3.5E 3.6A	1 3
5. Ensure users and system support personnel have the required security clearances, authorization, and need-to-know; are indoctrinated; and are familiar with internal security practices before access to the information system is granted.	1F 3.4F 3.5F	1 b 2 4

Table A-B-4. IAO Training Standards

<b>IAO Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4014</b>
6. Enforce security policies and safeguards on all personnel having access to the information system for which the IAO is responsible.	1D 2.2A	1 b 2 4 a, 4 c, 4 e 5 6 a 8 b 9 a
7. Serve as member of the CM board if designated by the IAM.	3.2E	6 b
8. Initiate protective or corrective measures to maintain security on information system.	2.1B 3.1C 3.2C 3.4D	1 b 6 a 7 9 a
9. Ensure warning banners are placed on all monitors and appear when a user accesses a system.	3.5F	1 b 2 a
10. Notify the IAM and DAA when changes occur on information system(s) that might affect accreditation/certification.	2.1A 3.4E 3.5E	
11. Report security incidents to the IAM/DAA in accordance with component guidance.	1D 3.5D	2 a 6 a, 6c 7 a 7 e 8
12. Report the security status of the accredited environment as required by DAA and update the SSAA, as the information system is modified or new components are added.	2.1A 3.4E 3.5E	1 b 3 b 9 10 d
13. Conduct periodic reviews to ensure compliance with the accreditation/certification support documentation package.	3.3E	3 a, 3 b
14. Follow procedures developed by the IAM, in accordance with CM policies and practices, for authorizing software use prior to its implementation on an information system.	3.2D 3.2E 3.3E	2 f

Table A-B-4. IAO Training Standards (cont'd)



<b>IAO Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4014</b>
15. Ensure support to IAVM requirements and ensure security patches are installed, as appropriate.	2.2D 2.2E 3.4D	
16. Ensure users and system administrators of the system(s) or network(s) are provided appropriate annual network security training.	3.5A	

Table A-B-4. IAO Training Standards (cont'd)

c. Table A-B-5 provides applicable national training standards in NIST Standard #800-16 (reference o) for IAM responsibilities in Appendix A.

<b>IAM Responsibilities</b>	<b>NIST Standard # 800-16</b>
1. In conjunction with the program manager, maintain for the DAA the SSAA to document site security improvements and progress towards meeting and maintaining accreditation of information systems.	2.1A 3.4E 3.5E
2. Implement the SSAA and provide security oversight at single or multiple sites or networks as directed by the DAA.	2.1A 2.2A
3. Coordinate security measures including analysis, periodic testing, evaluation, verification, accreditation, and review of information system installation at the appropriate classification level within the command or organization network structure.	1E 3.1A 3.2D 3.5C
4. Ensure security instructions, guidance, and SOPs are prepared, maintained, and implemented by each site.	2.1C 2.2A 2.2C
5. Develop and implement an information system security program.	2.1D
6. Review the SSAA to confirm that the residual risk is within acceptable limits.	3.1F
7. Oversee all IAOs to ensure that they receive proper technical training and information system policies and procedures are followed.	3.5A

Table A-B-5. IAM Training Standards

<b>IAM Responsibilities</b>	<b>NIST Standard # 800-16</b>
8. Ensure IAM/IAO and SAs review weekly alerts, bulletins, and advisories that impact security of site information systems to include DOD CERTs, ACERTs, AFCERTs, NAVCIRTs, MARCERTs and IAVAs.	2.2D 2.2E 3.4D
9. Develop reporting procedures and report security violations and incidents to the DAA and local management, as appropriate.	2.1C 2.2C
10. Monitor implementation of security guidance and direct action appropriate to remedy security deficiencies.	1D 2.2A 2.2D
11. Ensure that procedures are developed and implemented in accordance with CM policies and practices for authorizing use of software on information systems. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the IAM or IAO and approved by the DAA prior to changes. Routine system modifications and IAVA implementation may be preauthorized by the DAA within the SSAA.	3.3E
12. Serve as member of the CM board or delegate this responsibility to an appropriate IAO.	3.2E 3.3E
13. Ensure users and system support personnel have the required security clearances, authorization, and need to know and are indoctrinated on organization security practices before granting access to the information system.	1F 3.4F 3.5F
14. Ensure audit trails (system logs) are reviewed periodically (daily or weekly) and audit records are archived and maintained for future reference in compliance with local policies.	1F 3.4F 3.5F
15. Ensure data ownership and responsibilities are established for each information system, to include accountability, access, and special handling requirements.	1F 3.4F 3.5F
16. Maintain a repository for all system accreditation or certification documentation and modifications.	3.3E 3.4E
17. Advise the DAA.	
18. Ensure IAO (or network security officer) are appointed for all information systems and networks within the cognizance of the DAA. In the absence of an IAO, the IAM will act in that capacity.	

Table A-B-5. IAM Training Standards (cont'd)

<b>IAM Responsibilities</b>	<b>NIST Standard # 800-16</b>
19. Attend periodic IAM-level information systems security training as required.	
20. Ensure that system users are provided annual IA awareness training, and system administrators, management, and network security personnel are provided appropriate systems security training for their duties.	1F 3.5A

Table A-B-5. IAM Training Standards (cont'd)

d. Table A-B-6 provides applicable national training standards in NIST Standard #800-16 (reference o) and NSTISSI No. 4012 (reference q) for DAA responsibilities in Appendix A.

<b>DAA Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4012</b>
1. Ensure a properly conducted certification is accomplished on each system considered for accreditation in accordance with DITSCAP.	3.2E	2 j, 2 n, 2 p 5 a 9 11 b
2. Issue written accreditation statement after formal review of the SSAA. Including the certification report issued by the CA	3.2E	2 j, 2 n, 2 p 5 a 9 11 b
3. Grant final and interim accreditation of network in a specified security mode.	3.2E	8 b 11 a, 11 b, 11 c
4. Ensure that security is incorporated as an element of the information system life-cycle process.	3.2E 3.3E	9 a, 9 b
5. Delegate accreditation approval authority, if necessary or desirable.	1A	2 n 5 b

Table A-B-6. DAA Training Standards

<b>DAA Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4012</b>
6. Review the SSAA to confirm that the residual risk is within acceptable limits.	3.2E	3 11 a, 11 b, 11 c
7. Verify that each SSAA complies with the information system security requirements, as reported by the IAM. Ensure the operational information security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.	3.4E 3.5E	2 m, 2 n, 2 o
8. Ensure the establishment, administration, and coordination of security for systems that the DAA's command or organization operates.	2.1D 3.3E	2 a, 2 d, 2 f, 2 g, 2 j, 2 k, 2 l, 2 m 6 b 10
9. Ensure records are maintained for all information system accreditation/certifications under DAA's purview, to include use of IA tools.	3.2E 3.3E	2 j, 2 n, 2 p 5 a
10. Ensure that an incident reporting program is established and security incidents are reported to affected parties, data owners, etc.	1A 2.1D	1 c 2 o 3 i 5 a
11. Ensure that the program manager, in conjunction with the IAM and IAO, define the system security requirements for acquisitions in the SSAA.	3.4E	1 e 2 i 4 7 b 10 b, 10 c, 10 f 11 c
12. Assign security responsibilities to the individuals reporting directly to the DAA (e.g., IAM and IAO).	1A 2.1C	8 a
13. Approve the classification level required for applications implemented in a network environment.		1 d, 1 f, 1 l 3 b, 3 d 6 a 8 b

Table A-B-6. DAA Training Standards (cont'd)

<b>DAA Responsibilities</b>	<b>NIST Standard # 800-16</b>	<b>NSTISSI # 4012</b>
14. Ensure DSAWG approved additional security mechanisms necessary to interconnect to external systems at different classification levels (e.g., encryption and guards) and comply with connection procedures.	3.2E 3.3E	2 j 8 b 11 c
15. Ensure that criticality and sensitivity levels of each network, site, system, or application are identified in the SSAA.	3.3E	2 n
16. Review the SSAA to ensure each information system supports the security requirements as defined in the network, site, system, or application and network security programs.	3.3E 3.5E	2 j, 2 m
17. Ensure that organizations plan, budget, allocate, and spend resources to achieve and maintain an acceptable level of security and to remedy security deficiencies.	2.1D	5 b 9 a
18. Ensure that a security education, training, and awareness program is in place and actively supported.	3.5A	
19. Ensure counter-intelligence activities are considered during the certification and accreditation process.		
20. Establish working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in MOA.		8 b
21. Ensure that when classified or sensitive-but-unclassified information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as cryptography, and PDS.		2 j, 2 m
22. Appoint the IAM, in writing, to act as the chief technical IA advisor.		

Table A-B-6. DAA Training Standards (cont'd)

(INTENTIONALLY BLANK)

APPENDIX C TO ENCLOSURE A  
IA ORGANIZATIONS ROLES AND MISSIONS  
TO BE PUBLISHED

(INTENTIONALLY BLANK)



## ENCLOSURE B

## DEFENSE-IN-DEPTH OPERATIONS

## INTRODUCTION

1. IA policy drives operations by establishing goals, actions, procedures, and standards.
2. Defense-in-depth requires a widely distributed intrusion detection effort to recognize and describe activities that are different from the normal pattern or fit known "bad" patterns, and to limit and contain the access across networks that a malicious user may exploit. The nature and scope of the incident, effects, cause, and vulnerability must be determined. After an intrusion is detected, incident information must be reported through established channels to appropriate authorities and specialized analysis and response centers. Incident response begins with immediate local emergency damage-limitation and survivability actions that should be stated in organizational information systems security policy, procedure, tactics, and training guidance (e.g., SOPs, contingency plans, etc.) and implemented promptly. Appendix B of this enclosure, "Incident and Vulnerability Reporting," provides guidance, procedures, and formats on incident reporting for the Department of Defense.
3. Computer network operations, to include defense-in-depth operations, are crucial activities for assuring network access, information, and network protection, and information delivery at strategic, operational, and tactical levels. As such, these operations have received increased emphasis within the combatant command headquarters. Joint force commanders at all levels are becoming aware that the number and complexity of networks within their area of operations is rapidly outstripping their ability to understand and manage information flows, provide network management, and protect the information and the networks that carry it against intrusions and attacks. For these reasons, DOD network operations policy recognizes the need for network operations and security centers (NOSCs) operated by the combatant commands. These theater coordination and/or control centers link together widely dispersed Service and agency NOSCs through a command and organizational relationship. They establish joint tactics, techniques, and procedures to ensure a joint procedural construct and establish a technical framework to create a common network picture for the joint force commander. Equally important to a common network picture is the ability to use common software applications and tools, approved through established mechanisms and accepted by all enclaves. Approved software must be easy to install, upgrade, and maintain on a worldwide basis if need be. Every effort to accept useful applications and tools without redundant testing by individual enclaves is essential to success of all combatant commands Services and agencies.

25 March 2003

4. Commanders must be provided with a fused assessment of computer network attacks (CNAs) against DOD networks and a coordinated process that integrates analysis from the operational, intelligence, counterintelligence, and law enforcement communities. Analysis of incident data reported by the CERT community in accordance with CJCSM 6510 has threat warning value for identifying imminent, underway, or potential long-term strategic CNAs against DOD networks. Network incident data contains indications of adversary reconnaissance, probing, intrusion, and network exploitation and/or attack activity. Long-term coordinated analysis is extremely important when distributed, coordinated, low-visibility, network-based attacks occur across many systems over an extended period. Designated intelligence and law enforcement entities must maintain awareness of potential hostile organized state or nonstate-actor CNA, computer network exploitation (CNE) or other information operations (IO) activities and capabilities to provide timely warning of impending or ongoing hostile operations. Careful, effective, and timely decisions must be made concerning appropriate additional responses such as declaring a higher-level security posture (i.e., increasing INFOCON, isolating affected elements, or pursuing legal, diplomatic, economic, or military actions). Skillfully integrated IO counterattack or counteroffensive actions can contribute significantly to the overall defensive effort. Appendix C of this enclosure, "Information Operations Conditions," provides a summary of DOD implementation of INFOCONs with specific guidance, procedures, and guidance found at the USSTRATCOM West SIPRNET website (<http://www.usspace.spacecom.smil.mil/SJ3/sj39/index.htm>). INFOCON system will be integrated into a future change to CJCSM 3402.01B, "Alert System of the Chairman of the Joint Chiefs of Staff" (reference r).

5. Response measures must also ensure information systems essential to performing critical missions are not crippled by unacceptable interruption, and vulnerabilities are closed. Appendix A of this enclosure, "Information Assurance Vulnerability Management Program," provides guidance, procedures, and IA vulnerability formats (i.e., IAVAs, IAVBs, and IA technical advisories (TAs)).

6. Initial guidelines and considerations for Joint IA Red Team operations conducted against joint information systems and networks are provided in Appendix D of this enclosure, "Joint IA Red Team Operations."

APPENDIX A TO ENCLOSURE B

INFORMATION ASSURANCE VULNERABILITY MANAGEMENT PROGRAM

1. Information Assurance Vulnerability Management Program (IAVM) Program

a. The Information Assurance Vulnerability Alert (IAVA) process (instituted by the Department of Defense in 1998) provides positive control of vulnerability notification, corresponding corrective action and IAVA status visibility for DOD network assets. The IAVM program supersedes the previous IAVA process. This change represents a transformation in the program course focusing on the status of DOD networks to mitigate or eliminate known vulnerabilities.

b. This appendix establishes responsibilities and procedures for the IAVM program. This includes organizational and individual accountability, responsibilities, generation process, registration, compliance criteria, reporting, enforcement, validation, and verification.

c. The DOD IAVM program process includes three types of vulnerability notifications:

(1) IAVA. An IAVA addresses severe network vulnerabilities resulting in immediate and potentially severe threats to DOD systems and information. Corrective action is of the highest priority due to the severity of the vulnerability risk.

(2) IAVB. An Information Assurance Vulnerability Bulletin (IAVB) addresses new vulnerabilities that do not pose an immediate risk to DOD systems, but are significant enough that noncompliance with the corrective action could escalate the risk.

(3) TA. A Technical Advisory (TA) addresses new vulnerabilities that are generally categorized as low risk to DOD systems.

2. Applicability and Scope. The IAVM program applies to any device on any DOD owned or controlled information system network, to include but not limited to workstations, servers, routing devices (router, switch, firewall), networked peripherals (e.g., network printers, portable electronic devices) and controlled interfaces (e.g., guards). A device is considered a single node on a network if it has its own network identification (internet protocol (IP) and/or media access control address).

3. Individual and Organization Accountability for Implementing IAVM Program. Combatant commands, Services and agencies (CC/S/As) will ensure individual and organization accountability for implementing the IAVM program and protecting information systems.

a. Individual commanders, designated approving authorities (DAAs), managers, supervisors and administrators are responsible and accountable for ensuring the implementation of the DOD IAVAs, IAVBs and TAs actions.

b. Military and civilian personnel (including contractors) will be subject to administrative and/or judicial sanctions if they knowingly, willfully or negligently compromise, damage or place at risk DOD information systems by not implementing the DOD IAVAs and directed IAVB and TAs in accordance with this manual and supplemental CC/S/A policies and procedures.

c. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access. Action may also be taken under the Uniform Code of Military Justice (UCMJ) and applicable federal or state law.

#### 4. IAVM Asset Compliance Status

a. IAVM compliance reporting will be reported for applicable asset type, which are:

(1) Critical Servers and/or Infrastructure Components. A specific subset of components identified in each CC/S/A enterprise designated as both critical and at high risk. These assets must be protected as a first priority due to the potential severe negative impact of their loss or exploitation on operational readiness of DOD assets. The Joint Task Force-Global Network Operations (JTF-GNO) (enterprise-wide) or CC/S/A headquarters (CC/S/A wide) will identify critical servers and/or infrastructure components.

(2) Servers and Infrastructure Components. Core servers (e.g., domain controllers, E-mail servers, etc.), infrastructure components (e.g., routers, switches, etc.), and functional servers (e.g., program management office-managed, major command-unique, etc.).

(3) Workstations. End user workstations, to include both desktops and laptops.

b. Applicable assets are reported in one of three compliance status levels.

(1) Operating assets that are not patched, are vulnerable, and at risk for exploitation.

(2) Operating assets that are not patched but have CC/S/A approved and implemented mitigation plans to reduce risk.

(3) Operating assets that are patched or have permanent fixes that removes risk, and compliance is reported to appropriate CC/S/A authority.

c. From the date an IAVA is issued the CC/S/A will report IAVA compliance status for assets:

(1) Upon an IAVA vulnerability notification, all affected assets will be placed in a noncompliant status.

(2) As implementation efforts progress, the asset status will change to implemented mitigation plan or patched and/or permanent fix.

d. Only IAVA statistics are reported using the Vulnerability Management System (VMS) IAVA Web application (see paragraph 14). The purpose is to show the compliance by asset type and overall status of DOD networks from the date the IAVA is released.

e. Mission Assurance Category (MAC). CC/S/A are required to assign a mission assurance category to their information systems in accordance with (IAW) with DOD Instruction 8500.2 (reference w). The mission assurance categories are primarily used to determine availability and integrity. Mission assurance categories will be used in support of IAVM program to identify **critical servers and/or infrastructure components** and setting IAVA implementation priorities for CC/S/A systems.

f. CC/S/A are strongly encouraged to adopt a similar IAVM compliance and overall status reporting process for directed IAVBs and TAs.

## 5. Organization Responsibilities

a. The Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)) has overall responsibility for the implementation of the IAVM program policy and procedures across all CC/S/As.

10 August 2004

b. The Director, Command, Control, Communications and Computer Systems (J-6), Joint Staff, will develop Joint IAVM program policy and guidance in coordination with the Joint Staff (J-3 and J-2), USSTRATCOM, and other CC/S/As.

c. Commander, US Strategic Command (CDRUSSTRATCOM), will:

(1) IAW CJCSI 6510.01D, Appendix C, paragraph 3, maintain overall responsibility for IAVM program execution.

(2) Report IAVA significant compliance issues concerning DOD organizations or incidents to the Chairman of the Joint Chiefs of Staff (Chairman) and the Secretary of Defense through the Joint Staff/J-6 and ASD(NII).

(3) IAW CJCSI 6510.01D, Appendix D, paragraph 6, direct corrective actions for enclaves or affected systems not in compliance with IAVM program.

(4) Develop common standards for IAVM program reporting.

(5) Through Commander, JTF-GNO, will:

(a) Monitor relevant sources of information to discover security conditions that may require IAVM vulnerability notification (IAVA, IAVB, and TA).

(b) Assess risk and potential operational impact associated with software vulnerabilities and develop IAVM vulnerability notification.

(c) Coordinate potential IAVM vulnerability notification with CC/S/As, if possible.

(d) Approve and publish IAVM vulnerability notifications.

(e) Monitor IAVA compliance and asset status across the Department of Defense.

(f) Conduct random and directed verification of CC/S/A IAVA compliance and status.

(g) Notify CC/S/As found noncompliant, direct corrective action, and verify those CC/S/As have acted to correct IAVA

10 August 2004

noncompliance under their authority for computer network defense (CND) (see paragraph 11).

d. Director, DISA, will:

(1) Implement and maintain an IAVA compliance and status tracking system to maintain IAVM program compliance statistics throughout the Department of Defense.

(2) Develop technical operations and engineering improvements to the IAVM program, to include capability to support joint/combined reporting and review of compliance status between combatant commands, Services, program managers and components.

(3) Provide technical support and engineering capability to the Service CERTs/CIRTs and or CND Service providers.

e. CC/S/As will:

(1) Implement an IAVM program that provides responsive and effective vulnerability management.

(2) Develop IAVA implementation procedures and processes including timelines, mitigation plans (including approval authorities), organization and individual responsibilities, organization and individual accountabilities, reporting requirements to vulnerability exploitation.

(3) Develop IAVB and TA implementation procedures and processes including timelines, organization and individual responsibilities, organization and individual accountability, reporting requirement and actions in response to vulnerability exploitation.

(4) Utilize DOD provided enterprise-wide or interoperable CC/S/A-procured automated tools and solutions for CC/S/A IAVM programs.

(5) Designate a primary and secondary representative responsible for managing its internal IAVM program. Register primary and secondary points of contact (POCs) in the VMS IAVA Web application (see paragraph 6).

(6) Acknowledge receipt of the IAVA or IAVB messages as directed in IAVM vulnerability notification.

(7) Disseminate vulnerability notifications to all subordinate organizations within the CC/S/A, to include, but not be limited to, program managers (i.e., joint and/or CC/S/A-specific programs), IAMs, IAOs, SAs, and/or other personnel responsible for implementing and managing responses to information system vulnerabilities. Joint programs are those programs centrally managed by one CC/S/A, but utilized by more than one DOD component and/or may be deployed enterprise-wide throughout the Department of Defense.

(8) Ensure all subordinate organizations comply with all IAVAs or develop and implement mitigation plans following CC/S/A guidance.

(9) Ensure all subordinate organizations comply with IAVBs and TAs IAW CC/S/A guidance.

(10) Report compliance by assets and overall status of all IAVAs via the appropriate VMS IAVA Web application as specified in the individual IAVA notification. Ensure combatant commands have visibility into Service and Defense agency components that support their operations.

(a) Update the VMS IAVA Web application (including noting no change) every 72 to 96 hours (twice weekly) until all assets are fixed or mitigation plans implemented.

(b) Update the VMS IAVA Web application as required (e.g., change in assets) when all assets are fixed (patched or permanent fix implemented).

(c) Include CC/S/A program manager reports for CC/S/A managed joint or CC/S/A specific programs in the CC/S/A overall report.

(11) Ensure risk mitigation actions are implemented (proactive or preventive actions/measures to mitigate vulnerability) or asset is blocked/disconnected if an IAVA cannot be implemented or mitigated (see paragraph 9).

(12) Maintain positive configuration control of all information systems and/or assets under their purview. As part of this process, ensure application of all active IAVAs to all systems (operating or deployed from storage for operations). Testing must be conducted to ensure IAVAs will not impair system operations.



(13) Maintain configuration documentation that identifies specific system and/or asset owners, IAMs, IAOs, and SAs.

(14) Ensure the verification of corrective actions on networked assets by both CC/S/A chain of command and independent authorized organizations.

(15) Establish a process to ensure that all DOD contracts for assets and services that fall within the scope of the IAVM program reflect the requirement of the IAVM program. This includes contracts in development that are IT-related and/or affect Global Information Grid (GIG) assets (uses, administers, or integrates IT and/or communication assets into the GIG).

(16) Monitor the implementation and/or mitigation plans for centrally managed CC/S/A programs via the VMS IAVA Web application, and disseminate the specific fix plan information to subordinate activities.

(17) Conduct IAVA program compliance checks of their subordinate organizations.

(18) When amplifying and /or referencing an IAVA, CC/S/As will include the original IAVA/IAVB vulnerability notification number in their message (e.g., Air Force C4 Notice to Airman related to a DOD IAVA will reference the related DOD IAVA number).

## 6. Individual Responsibilities

a. Designated CC/S/A IAVM representatives will:

(1) Register with DISA for assignment of user ID and password for access to the VMS IAVA Web application.

(2) Disseminate IAVM vulnerability notification to lowest level IAMs, IAOs, and SAs.

(3) Enter their organization's compliance data into the VMS IAVA Web application.

(4) Monitor IAVA compliance status and update the VMS IAVA Web application at least weekly until assets are fixed.

b. Program managers of centrally managed CC/S/A level or joint programs will:

10 August 2004

- (1) Establish a capability to implement or effectively mitigate the risk posed by critical vulnerabilities as identified in IAVA notifications.
- (2) Designate a primary and secondary IAVM POCs.
- (3) Respond to each IAVM vulnerability notification as the system configuration manager.
- (4) Register with DISA for a user ID and password for access to the VMS IAVA Web application. Note: Applies to CC/S/A Joint program managers. CC/S/A program managers may also register with DISA if authorized by designated CC/S/A IAVM representatives.
- (5) Acknowledge receipt of the IAVM vulnerability notification through the VMS IAVA Web application as directed in IAVM vulnerability notification. Note: Applies to joint program managers. CC/S/A program managers may also register with DISA if authorized by designated CC/S/A IAVM representatives.
- (6) Publish a program implementation or mitigation plan for every DOD IAVM notification issued. The program plan will provide an initial status and information required in paragraph 7.
- (7) Provide, if applicable, an implementation or mitigation plan for users of the joint program via the DISA VMS IAVA Web application. Provide an implementation or mitigation plan via CC/S/A equivalent VMS IAVA Web applications as required. Implementation or mitigation plans will address specific actions taken to implement patch or mitigate risks identified in IAVA messages. CC/S/A will note program and CC/S/A assets noncompliant due to lack of program implementation or mitigation plan.
- (8) Report asset compliance and overall status of all IAVAs via the appropriate VMS IAVA Web application as specified in the individual IAVA notification.
  - (a) The VMS IAVA Web application will be updated (including noting no change) every 72 to 96 hours (twice weekly) until all assets are fixed or mitigation plans implemented.
  - (b) Update the VMS IAVA Web application as required (e.g., change in assets) when all assets are fixed (patched or permanent fix implemented).

10 August 2004

(9) Ensure dissemination of the implementation or mitigation plan, if necessary, to affected SAs.

(10) Develop guidance for CC/S/As using centrally managed programs on IAVA implementation.

c. DAAs will:

(1) Ensure IAVM vulnerability notification messages are disseminated to the lowest level IAMs, IAOs, and SAs as required.

(2) Ensure all organizations comply with all IAVA directed actions.

(3) Review and submit in accordance with CC/S/A guidance and timelines a mitigation plan (including implementation timelines) if unable to comply with an IAVA. If unable to submit the mitigation plan following CC/S/A guidance and timelines the CC/S/A DAA will order the affected assets blocked or disconnected from the network.

(4) Monitor IAVA compliance and overall status for those assets under their control and ensure compliance reporting is accomplished to the appropriate CC/S/A reporting server (e.g., Service IAVM database).

(5) Ensure compliance checks of their organizations to validate mitigating and/or corrective actions are completed.

(6) Maintain positive configuration control of all information systems and/or assets under their purview. Maintain configuration documentation that identifies specific system and/or asset owners, IAMs, IAOs, and SAs.

(7) Ensure corrective actions on networked assets can be verified by both CC/S/A chain of command and authorized independent organizations IAW CC/S/A guidance.

d. IAMs and IAOs will:

(1) Advise and assist DAA on IAVM program.

(2) Monitor IAVM vulnerability notification messages.

(3) Monitor mitigation plans and implementation timelines as required.

(4) Maintain a list of IAVAs applicable to their systems by asset type.

e. SAs will:

(1) Ensure all devices are IAVA compliant, by applying all applicable IAVAs, prior to connecting the devices to any DOD owned or controlled information systems network.

(2) Respond to all active IAVAs. Any asset found noncompliant will be brought into immediate compliance. If the system cannot be brought into compliance, a mitigation plan will be developed and approved following CC/S/A guidance and timelines. If mitigation plan is not approved, then the system must be blocked or disconnected from the network.

(3) Monitor for new vulnerability notices.

(4) Report compliance information through CC/S/A specific channels to IAMs for aggregation and reporting.

(5) Report PM managed programs as IAVA noncompliant until IAVA directed implementation or mitigation actions are applied.

## 7. IAVM Vulnerability Notifications

a. The IAVM program process is implemented by using the IAVM vulnerability notification. Once a vulnerability is evaluated and warrants notification, JTF-GNO will publish the IAVM vulnerability notification, including one of the three following notifications and amplifying information.

(1) IAVA. IAVAs go into effect upon issuance.

(a) The JTF-GNO will direct actions to mitigate the risks associated with these vulnerabilities. Due to the severity of the risk presented by these vulnerabilities, corrective action is of the highest priority.

(b) CC/S/As will acknowledge and comply with directed actions listed in the IAVM vulnerability notification. Acknowledgment and compliance with corrective action is tracked and reported by each CC/S/A.

(c) IAVA notifications will be disseminated down to the IAM, IAO, and SA level within an organization.

(2) IAVB

(a) CC/S/As acknowledge receipt of the IAVB vulnerability notification.

(b) The local commander makes compliance requirements and decisions, as well as local reporting requirements.

(c) IAVB notifications will be disseminated down to the IAM, IAO, and SA level within an organization.

(3) TA

(a) Potential escalation of these vulnerabilities is deemed unlikely, but the advisories are issued so that any risk of escalation in the future can be mitigated.

(b) Reporting is not required in response to a TA.

(c) TA notifications will be disseminated down to the IAM, IAO, and SA level within an organization IAW within CC/S/A guidance.

b. Revisions to Vulnerability Notifications. The JTF-GNO will routinely issue revisions to vulnerability notifications based on new information (i.e., patch availability). JTF-GNO will update IAVM Web site to identify notices that have been updated. IAMs, IAOs, and SAs must review this Web site at least weekly to review updated notices. CC/S/A POCs are responsible for dissemination of revisions as appropriate. Receipt acknowledgement is not required.

c. Expiration of Vulnerability Notices. Vulnerability notices normally do not expire. Vulnerability notices may be superseded or modified, as supplemental technical information becomes available. In such cases, JTF-GNO will provide new acknowledgement and compliance requirements if necessary. In such cases the superseded notice will expire.

d. Numbering of Vulnerability Notifications. The vulnerability notifications are numbered to reflect the type and sequence. There may be cause to update an existing IAVA. There are two types of updates made to IAVM notices. Minor updates are made to update a link or clarify an issue but have no significant impact for systems or compliance.

Major updates are done when a significant change is made to a notice that may affect systems or compliance. No additional acknowledgment or compliance is required for minor updates. All minor updates are posted on the DOD CERT IAVM page. Newly identified patches, addition of major systems to vulnerable list, or important vendor specific information may trigger a major update. When a major upgrade to an IAVM notice is done, the notice is reissued to the Department of Defense in the same way a new notice is released. Additional acknowledgement and compliance instructions will be provided by JTF-GNO on a case-by-case basis. Note: IAVM notices are updated frequently. Due to the dynamic environment, it would be extremely difficult for organizations other than the JTF-GNO (DOD CERT) to host up to date IAVM notices. Therefore, the JTF-GNO (DOD CERT) is the only organization authorized to host DOD IAVM notices. Update information is posted on the JTF-GNO (DOD CERT) Web site. The format for the vulnerability notification number is as follows (Figure B-A-1):

<b>YYYY-T-####.V (i.e., 2001-A-0008)</b>	
<b>Legend:</b>	Description
<b>YYYY</b>	Year
<b>T</b>	Type of message <b>"A"</b> = Alert <b>"B"</b> = Bulletin <b>"T"</b> = Technical Advisory
<b>####</b>	Sequence number of the vulnerability notice
<b>V</b>	Version number if the vulnerability notice has been updated

Figure B-A-1. Vulnerability Notice Number Format

8. IAVM Program Process Flow

a. New vulnerabilities are identified or reported to the JTF-GNO. The JTF-GNO, determines if the vulnerability rates an IAVM vulnerability notification.

b. The JTF-GNO coordinates with USSTRATCOM, NSA, and other CC/S/As on potential new vulnerability notification. IAVAs go into effect upon issuance.

c. JTF-GNO develops the technical information regarding the vulnerability addressed in an IAVA notification message, and posts this on the JTF-GNO (DOD CERT) website (both SIPRNET and NIPRNET).

d. The JTF-GNO, in coordination with DISA, transmits the vulnerability notification via the CC/S/A command channels to the

10 August 2004

CC/S/A POC organization. JTF-GNO (DOD CERT) will also send notification message to all registered IAVA users via E-mail. The message will direct all recipients to review the technical information (patch or implementation plan) posted on the DOD CERT website, disseminate it to all subordinate activities, and acknowledge receipt as directed in vulnerability notification.

e. The CC/S/A POCs will access the JTF-GNO (DOD CERT) Web sites below to review technical information and assess the impact on their organizations.

(1) NIPRNET (<http://www.cert.mil>)

(2) SIPRNET (<http://www.cert.smil.mil>)]

f. The CC/S/A POC disseminates the alert information via command channels to all CC/S/A specific program managers, SAs, and/or other personnel responsible for implementing and managing technical responses to the alert.

g. The CC/S/A POCs acknowledge receipt of the vulnerability notification through the VMS IAVA Web application.

(1) CC/S/A POCs will acknowledge all IAVAs and IAVBs. The universal resource locators (URLs) for the server are as follows:

(a) NIPRNET: <https://vms.disa.mil>

(b) SIPRNET: <https://iava.disa.smil.mil/> or <https://vms.disa.smil.mil>

(2) To obtain a user ID and password for the VMS IAVA Web application, contact the Defense Enterprise Computing Center (DECC) Detachment, Chambersburg Helpdesk, at Defense Switched Network (DSN) 570-5690 or (717) 267-5690.

(3) Acknowledging receipt of a vulnerability notice indicates that the POC has read the message and has disseminated the information through command channels to the system (network) administrators.

h. Implementation of IAVA.

(1) As directed by the IAVA message and the chain of command, the SAs take corrective action on vulnerabilities and report compliance status through command channels to the CC/S/A POC.

(2) Joint program managers will:

(a) Acknowledge receipt of the vulnerability notice through the VMS IAVA Web application.

(b) Provide an initial status and an implementation or mitigation plan for users of the program via the VMS IAVA Web application. The program plan will provide specific implementation instructions to their respective CC/S/A IAVM POCs. The initial plan shall include advising customers that the PM has acknowledged the alert and provide a schedule for program compliance. CC/S/A POCs will publish updates to the plan as program specific path/ fix/ update/ workaround procedures are developed and directed by the PM.

(c) Ensure dissemination of the fix, if necessary, to affected SAs. Organizational POCs will report PM managed programs as IAVA-not compliant until such time as IAVA directed mitigation plan actions are applied.

i. The CC/S/A POC aggregates compliance information using Figure B-A-3 using the following governing tenets:

(1) The Services and agencies provide and account for the majority of the systems for the Department of Defense. However, combatant commands must have visibility into Service and Defense agency components that support their operations. Combatant commands will provide guidance to their components on information reporting requirements.

(2) The local network service provider is responsible for providing a secure environment for all users and, as a result, requires visibility on uncorrected vulnerabilities to their network assets.

(3) DOD entities will follow the chain of command reporting relationships as described in Figure B-A-3. These guidelines enable comprehensive compliance reporting of all DOD assets and prevent duplicate reporting of assets. Figure B-A-3 also enables the proper reporting to information addressees.

(4) Asset owners will identify the column of Figure B-A-3 best describing their organization. Each row of the matrix describes the actions to be executed by the owner and the relevant chain of command for that action. If Figure B-A-3 information does not apply to a specific unit or agency, then that unit or agency should refer to their domain



name (e.g., af.mil, army.mil, or stratcom.mil) and report to that entity. In other words, the domain name becomes the “tie breaker.”

(5) Column Definitions

(a) Organic/Assigned Forces and Same-Service Tenants. Organizations organic or assigned to a CC/S/A major command/headquarters that operate the base infrastructure or same Service.

(b) Other CC/S/A Tenants on Base Network. Tenants not part of the Service that operates the base infrastructure.

(c) CC/S/A Elements Not Connected to a Base Network. Organizations that, through geographical location or network connectivity separation, do not use a base service provider or that use host-base networks strictly for transport.

(d) Centrally Managed Systems (PM). Systems used throughout the Department of Defense or a CC/S/A whose configuration is centrally managed by a program office advocate for the CC/S/A to develop a similar structure matrix.

(6) Row Definitions

(a) Directed Action. The CC/S/A or program manager that directs specific IAVA compliance and reporting actions.

(b) Aggregated Reporting. These organizations collect individual asset statistics from bases, posts, camps, stations, and/or ships and report them to the IAVM program POCs, who in turn report them using the VMS IAVA Web application.

(c) Information Reporting. Organizations not in the reporting chain have an operational need to ensure their supporting units are IAVA-compliant.

j. The CC/S/A POC reports compliance statistics on the VMS IAVA Web application either through manual data entry or through the IAVA import file-upload feature.

(1) Report NIPRNET and SIPRNET compliance statistics separately. SIPRNET compliance statistics will only be reported on the SIPRNET VMS Web server (<https://vms.disa.smil.mil>). NIPRNET compliance statistics may be reported at either the NIPRNET or SIPRNET

10 August 2004

VMS Web servers. The SIPRNET VMS Web server provides separate data entry forms for NIPRNET and SIPRNET compliance statistics.

<b>Actions</b>	<b>Asset Owner/Program Manager</b>			
	Organic/ Assigned Forces and Same Service Tenants	Other CC/S/A Tenants on Base Network	C/S/A Elements Not Connected to a Base network	Centrally Managed Systems (PM)
Directed Action	Services	Parent CC/S/A ***	Parent CC/S/A	PM
Aggregated Reporting	Base Network Control Center (NCC) or equivalent	Parent CC/S/A	Parent CC/S/A	Parent CC/S/A****
Information reporting	CC*	Other supported CC* Agency** Base NCC	<b>Other Supported CC*</b> Agency**	Parent CC/S/A Base NCC
Note: * If organization supports a combatant command. ** In the case where an MOA has a CC/S/A tenant report to a service provider. *** Service tenant reports to parent Service while joint organizations and unit report (e.g., Joint Information Operations Center (JIOC)) to the supported combatant command. Every effort will be made to insure duplicate reporting of assets is not taking place. Where conflicts arise that are not covered by this matrix, the final decision will be determined by the domain name of the network. **** See paragraph 6.b.(4)				

Figure B-A-3. Reporting Chain of Command

(2) Compliance statistics are required for all IAVA. The initial status for an organization's compliance is noncompliant assets (Red). The CC/S/A IAVM POC will change the status to reflect the posture of the organization. Statistics will include 100 percent accountability of the registered computer assets affected by the vulnerability.

(3) There are three types of status that can be entered for an IAVA: "Not Applicable," "Unknown," (i.e., actual numbers not known) or "Statistics Provided." The following data will be provided in compliance reports for a status of "Statistics Provided" as shown in Figure B-A-4.

(4) Reporting of overall organization IAVA compliance level status is on criteria outlined in paragraph 4.

(5) Automated compliance tracking systems, such as the Vulnerability Compliance Tracking System (VCTS), report statistics on a near-real-time basis. During day-to-day operations, SAs constantly add and delete systems in their networks. If compliance data is extracted from the VMS IAVA Web application during the registration of new assets, some may be reported in the open category. During follow-up reporting, this status will be updated.

<b>Statistics</b>	<b>Definition</b>
# Assets Affected	Numbers of assets vulnerable.
# Assets in Compliance	Numbers of impacted assets implementing the solution.
# Assets with permanent fix	Number of assets implementing a permanent fix that removes risk of exploitation.
# Assets with mitigation plans	Number of assets with approved and implemented risk mitigation plan.
# Assets not compliant without mitigation plans	Number of assets that are not compliant and do not have an implemented risk mitigation plan or permanent fix.
Remarks	Add additional comments
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Report assets in one of three types: (1) Critical Servers and Infrastructure Components, (2) Servers and Infrastructure Components or (3) Workstations.</li> <li>2. Comments should explain how compliance was achieved.</li> </ol> <p>An audit file will be maintained of all transactions generated within the VMS IAVA Web application. Audit records will contain information concerning the transaction that occurred, a date/time stamp, and the userid that initiated the transaction.</p>	

Figure B-A-4. Compliance Reporting Data

k. The CC/S/A POC will maintain compliance statistics throughout the vulnerability notice life cycle.

1. CC/S/As will conduct compliance checks of subordinate organizations to ensure systems are IAVA compliant or have approved mitigation plans in place.

m. JTF-GNO will report the following to Headquarters, USSTRATCOM, for reporting to the Joint Staff:

(1) Significant IAVA compliance issues as identified for specific organizations and or incidents.

(2) Overall status for CC/S/As as directed. All report data will be extracted from the VMS IAVA Web application.

n. Periodically the JTF-GNO will publish IAVA revisions. These revisions will be posted to the JTF-GNO (DOD CERT) Web site and notices will be distributed to CC/S/A IAVM POCs.

9. Operating NonCompliant Assets Accountability and Responsibilities

a. Organizations and individuals operating noncompliant assets are accepting risks, accountability and responsibility for impacts internal and external to their networks in the event the vulnerability is exploited.

b. Commanders, organization directors and responsible individuals (e.g., DAA, IAM or IAO) will operate noncompliant assets only with mitigation plans IAW with CC/S/A guidance. USSTRATCOM will monitor IAW paragraph 10.

c. Noncompliant assets without mitigation plans will be disconnected, blocked or otherwise have the vulnerability removed IAW CC/S/A guidance. Vulnerable assets that remain operational with mitigation plans must be reported in the VMS IAVA Web application by the CC/S/A representative with the following data:

(1) System.

(2) Name of system.

(3) Description of system (short paragraph).

(4) Type of noncompliant assets (e.g., workstations, core-service servers, infrastructure components, etc.).

(5) IAVA number.

(6) Estimated date of completion.

(7) Reason system is not compliant.

(8) Risk assessment (high, medium, or low). Note: Risk assessment should address, as a minimum, the number of systems affected, indications and warnings (I&Ws) and potential operational impact of noncompliance.

(9) DAA name and contact information (Name, E-mail, telephone number).

(10) System POC (Name, E-mail, telephone number).

d. CC/S/A will develop guidance and timelines for approving mitigation plans for their subordinate organizations and agencies.

e. CC/S/A will develop guidance and timelines for approving permanent fixes including technical review of fix to ensure vulnerability cannot be exploited.

f. CC/S/A will monitor compliance and mitigation plans.

10. USSTRATCOM IAVA Compliance and Network Status Oversight

a. USSTRATCOM (JTF-GNO) will selectively monitor overall DOD compliance and overall status, mitigation plans and permanent fixes.

b. USSTRATCOM (JTF-GNO) may request information from CC/S/A CIO on noncompliant assets, mitigation plans or permanent fixes.

c. USSTRATCOM (JTF-GNO), in coordination with CC/S/As, can direct additional actions to mitigate risk for noncompliant assets including blocking or disconnecting assets. USSTRATCOM will coordinate with Joint Staff and CC/S/As to determine operational impact to Department of Defense before instituting blocking or disconnection.

11. Component NonCompliance Notification and Enforcement Procedures

a. If USSTRATCOM (JTF-GNO) determines that continued operation of noncompliant assets or current mitigation actions for assets is placing DOD networks at an unacceptable risk, USSTRATCOM (JTF-GNO) will notify CC/S/A IAVM authority (point of contact) to coordinate corrective actions.

b. If the DOD component fails to follow through with resolving its noncompliance, CDRUSSTRATCOM will release an IAVA noncompliance message (INFO ASD(NII)/IA and Joint Staff J-3 and J-6) addressed to the CC/S/A commander or director.

c. Noncompliant CC/S/As will respond within 96 hours that assets have been brought into compliance or report reasons for noncompliance, planned corrective actions, mitigation plan, and operational impact. CC/S/As will respond to CDRUSSTRATCOM (INFO ASD(NII)/IA, Joint Staff, J-3 and J-6 and JTF-GNO).

d. USSTRATCOM will review planned component corrective actions and coordinate or direct any additional actions (including blocking or disconnecting assets) required to mitigate vulnerability created by noncompliance IAW paragraph 5.12.5, DOD Directive O-8530.1 (reference s). USSTRATCOM will coordinate with Joint Staff and CC/S/As to determine operational impact to Department of Defense before instituting blocking or disconnection.

e. If USSTRATCOM finds noncompliant systems and networks that handle sensitive compartmented information, USSTRATCOM will inform the Defense Intelligence Agency (DIA) (SYS-4B) and NSA (V15).

f. If USSTRATCOM or DOD component has an issue that cannot be resolved concerning compliance actions, ASD(NII) and the Chairman will be informed.

(1) Combatant commanders will inform the Chairman.

(2) Defense agencies and DOD field activities will inform ASD(NII).

(3) Services will inform the Chairman and/or ASD(NII) as appropriate.

(4) ASD(NII) will notify and advise the Secretary of Defense on recommended course of action to resolve issue in coordination with the Chairman, CC/S/A, and CDRUSSTRATCOM.

## 12. IAVM Program Compliance Validation and Verification

a. The DOD Inspector General and CC/S/A inspectors general will include the IAVM program policies and compliance as a special inspection item.

b. DISA will conduct directed compliance checks of CC/S/A to verify IAVA compliance and mitigation actions in support of USSTRATCOM and all other combatant commands as requested.

c. CC/S/As must maintain an accurate status of IAVA compliance and status.

d. As changes are made to network configurations (hardware and software), CC/S/As will ensure that previously issued IAVAs are reviewed and re-implemented as appropriate. CC/S/As will also ensure that the VMS IAVA Web application accurately reflects all configuration changes.

e. CC/S/As will conduct independent or directed compliance verification assessments to ensure IAVA compliance and maintenance of accurate IAVA status in database.

### 13. Incident and Follow-Up Reporting

a. Incidents resulting from exploitation of IAVA vulnerability will be reported following incident reporting procedures, using the incident report format (Appendix B, Enclosure B).

b. CC/S/As will investigate and prepare an after-action report forwarded to USSTRATCOM (JTF-GNO) within 30 days providing:

(1) Cause for failure to implement IAVA or failure of mitigation action(s) to prevent exploitation of vulnerability (e.g., individual actions/inaction, procedural, or technical).

(2) Corrective actions taken (e.g., sanctions against individuals at fault or changes in CC/S/A procedures or processes).

c. JTF-GNO through Headquarters, USSTRATCOM, will provide to Joint Staff/J-6 a monthly summary of incidents resulting from exploitation of IAVA vulnerabilities including:

(1) Number of incidents by IAVA.

(2) Impacts of exploitation of IAVA vulnerability on the Department of Defense.

(3) CC/S/A reported cause and corrective action taken for previous reported exploitation of IAVA vulnerability.

d. Joint Staff/J-6 will disseminate to the Chairman, ASD(NII), and Service Chiefs as necessary.

14. Vulnerability Management System (VMS)/Vulnerability Compliance Tracking System (VCTS)

a. VMS/VCTS is a Web-based application designed to track compliance at the asset and administration level with the IAVM process. DISA developed the VMS/VCTS to address vulnerability management and to facilitate the notification of responsible parties of IAVAs. VMS/VCTS catalogs the receipt of IAVAs by asset, and tracks the compliance status of vulnerabilities. VMS/VCTS also incorporates accredited and program managed assets plan of action. VMS/VCTS provides:

- (1) A robust reporting capability, facilitating oversight and reporting for users appropriate to their organizational level.
- (2) Participating organizations with the ability to disseminate vulnerability notifications within their organization.
- (3) IAVA compliance statistics pushed to the VMS IAVA Web application.

VMS/VCTS is available for use by all combatant command headquarters, Joint, and sub-unified components, as well as to the Services and Defense agencies. DISA will provide VMS/VCTS training, implementation, and operational support to the VMS/VCTS users. Further information on VMS/VCTS and its use may be obtained by contacting the DISA Field Security Operations Office at DSN 570-9900.



## APPENDIX B TO ENCLOSURE B

## INCIDENT AND VULNERABILITY REPORTING

1. Incident and Vulnerability Reporting. This appendix provides joint guidance on incident and vulnerability reporting for DOD information systems. It also incorporates the National Security Information System Incident Program (NSISIP) strategy outlined in NSTISSD No. 503 (reference t).

a. The NSISIP focuses on security incidents and vulnerabilities threatening national security systems. This program is applicable to all USG departments and agencies and their contractors that acquire, develop, use, maintain, or dispose of national security systems.

b. The objectives of the NSISIP are to coordinate national security systems vulnerability and incident reporting and responses while facilitating:

(1) Cooperation among appropriate organizations and agencies in sharing incident, vulnerability, threat, and countermeasure information as well as information concerning national security systems.

(2) Effective and timely response to security incidents on national security systems.

(3) Development and use of incident-response methods, countermeasures, and technologies.

(4) Timely reporting of violations of law to appropriate law enforcement agencies.

c. Procedures established for incident response and vulnerability reporting for non-national security information systems must be integrated and compatible with NSISIP procedures.

d. Notification of incidents (probes and/or scans, intrusions, or malicious logic) against DOD non-national security systems also requires coordination among Services, Defense agencies, and other Defense components. Timely notification of incidents supports CND by initiating the response process and warning dissemination to users and information system administrators. CDRUSSTRATCOM, in coordination with the NSA, the Joint Staff, Services, and DISA, will develop policies and procedures for ensuring all incidents are reported through appropriate channels (e.g., operational report (OPREP) through operations channels or CRITIC through intelligence channels).

## 2. Incident Reporting Procedures

### a. Reporting Structure

(1) The incident reporting community is organized into multiple levels: global, regional, and local. All incidents and reportable events (defined in the following "Reporting Guidelines") will be reported to the DOD CERT. The DOD CERT will provide reports to JTF-CNO.

(a) Local Level. Local control centers (LCCs) are at Service component headquarters, major commands, and Service elements at a base, post, camp, or station (B/P/C/S) or joint activities that serve as a focal point for handling incidents and network management at the lowest level.

1. Service elements at B/P/C/S will report, through Service-defined channels, to the Service or agency CERT or CIRT, which will report to the DOD CERT for informational purposes and report operationally to their Service component of JTF-CNO.

2. Service elements subordinate to a commander of a combatant command will also be required to simultaneously report to a CERT or CIRT and/or combatant command theater coordination center, as directed by combatant command instruction or policy.

3. Joint activities will report incidents to their host command LCC, combatant command, and DISA regional CERT.

### (b) Regional Level

1. The RNOSCs and collocated regional CERTs (RCERTs) provide direct support to the regional combatant commands with RCERT and technical reporting. The RNOSCs (RNOSC-EUR (Europe), RNOSC-PAC (Pacific), RNOSC-CONUS (continental United States), and RNOSC-SWA (Southwest Asia)) are operated by DISA.

2. Service level: Service or Agency (CERT or CIRT; i.e., ACERT, AFCERT, NAVCIRT, DLA CERT, and MARCERT). Each Service has a CERT or CIRT. Some Service CERT or CIRT architectures also include organizational elements that support regional components for the respective combatant commands or major commands. Each Service and Defense agency CERT or CIRT providing CND services to a Service or Defense agency component supporting a regional combatant command will make available warnings, reports, information, data, and statistics pertinent to the protection of resources assigned to the regional combatant command. Regional Service and

Defense agency CERT or CIRT organizational elements will ensure that incident reports are provided to the respective regional combatant commands in addition to reporting to their Service or Defense agency CERT or CIRT.

(c) Global Level. The global level consists of the Joint Staff, USSTRATCOM, DISA Global Network Operations and Security Center (GNOSC), DOD CERT, NSA, National Security Operations Center Information Protection Cell (IPC) and National Security Incident Response Center, DIA, and the National Infrastructure Protection Center (NIPC). NIPC serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

(2) Information on computer or web anomalies and network incidents needs to be preserved to enable possible criminal prosecution.

(3) To increase situational awareness of overall network status, incident reporting and network management processes must be fully integrated. The incident reporting process augments existing operational reporting requirements through the chain of command OPREP or CRITIC reporting).

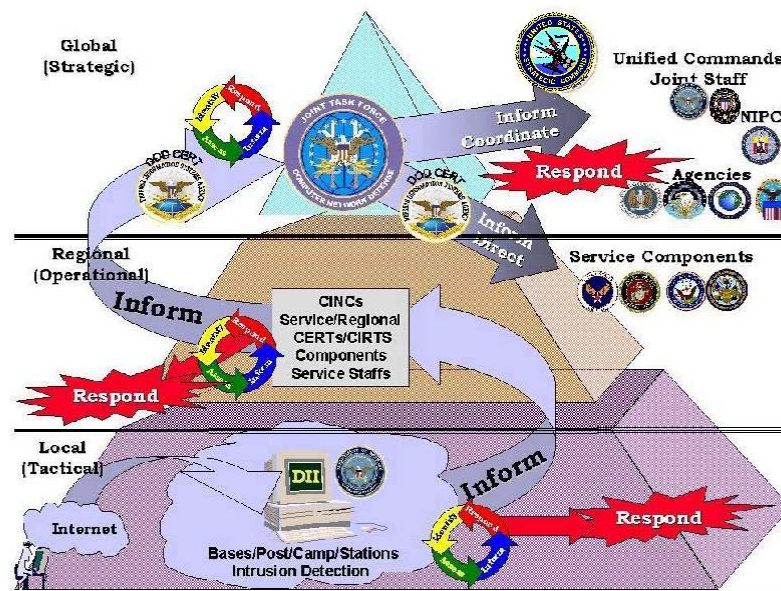


Figure B-B-1. Incident Reporting Structure

(4) Figure B-B-1 presents the flow of an incident report through the levels, demonstrating the recurring use of the process (identify, assess, inform, and respond) at each level.

(5) Analysis and correlation of event and incident data occur at all levels, as well as within various functional communities (e.g., intelligence, counterintelligence, law enforcement, and communications).

b. Reporting Guidelines

(1) Any user noticing anomalous or suspicious activity (incident or reportable event) will report the situation **immediately** to their help desk and/or SA, who will immediately notify the LCCs or CND service as outlined in local procedures.

(2) The commander's critical items of information (CCII) are a set of specific operational reporting criteria that enumerate unauthorized results, deemed by JTF-CNO to be the best indicators of an incident having strategic significance. They are intended to refine reporting requirements in this manual, and units that report incidents based on paragraph 2a above will have satisfied the reporting requirement. CCII are divided into priority 1 and 2 categories and will be periodically modified and updated to reflect, for example, a specific threat organization, vulnerability, virus, etc.

(3) Figure B-B-2 is an example CCII list. The current CCII list is maintained by the JTF-CNO and must also be maintained by all units required to report under CJCSI 6510.01C (reference b). Figure B-B-2 lists examples of reportable incident and event priorities for reporting the information to JTF-CNO through the DOD CERT, Service, agency, and regional channels.

(4) The entire CCII list is reviewed weekly by the JTF-CNO, and normally changes to the list will be published in message format. It is anticipated that the list will not change every week, and CCII messages will be serialized to ensure continuity.

(5) Any reporting unit may, through normal reporting channels, recommend CCII updates. Component commanders may add to this list for reporting Service-unique items of interest. The JTF-CNO is responsible for maintaining and updating the CCII list and publishing updates to reporting units in the form of a message.

<b>Priority</b>	<b>Reportable Incident/Event</b>
1       1 (continued)	<ul style="list-style-type: none"> <li>Any intrusion into a classified network with a perceived unauthorized result.</li> <li>Any ongoing unauthorized privileged user, administrator, or root level access of a DOD System.</li> <li>Any indications of Denial of Service or Distributed Denial of Service attacks.</li> <li>Any new virus or worm for which no published countermeasure exists, any new virus whose propagation could likely outrun DOD containment capabilities, or any new virus that affects network services (e.g., E-mail and domain name system (DNS) services).</li> <li>Any root level access on a system using new methods that exploit significant vulnerabilities shared by DOD systems.</li> <li>Any incident involving a second level domain web server (e.g., www.army.mil, www.dtic.mil, etc.)</li> <li>Any incident that negatively impacts ongoing military operations.</li> </ul>
<b>Priority</b>	<b>Reportable Incident/Event</b>
2	<ul style="list-style-type: none"> <li>Any incident(s) that cross C/S/A boundaries.</li> <li>Any intrusion of the Office of the Secretary of Defense networks.</li> <li>Any incident from a country against which the United States is currently conducting operations or will imminently conduct operations.</li> <li>Any intrusion of a tactical or deployed operational network.</li> <li>Any incident involving a NIPRNET or SIPRNET gateway (e.g., SIPRNET guard) or on a domain with a SIPRNET guard to include scans and probes.</li> <li>Any incident within a system that is shared by C/S/As (e.g., Global Command and Control System (GCCS), Global Combat Support System (GCSS), DMS, etc.)</li> </ul>

Figure B-B-2. Reportable Incident and Event Priorities

(6) All DOD agencies and other joint activities will report incidents (or reportable events) affecting collateral networks directly to the DOD CERT. All DOD agencies and other joint activities for which DIA is the cognizant security

25 March 2003

authority will report incidents (or reportable events) affecting the joint worldwide intelligence communications system (JWICS) to DIA. DIA will forward reports to the NSA Intelligence Community – Incident Response Center (IC-IRC) in accordance with established concept of operations (CONOPS). Guidance for reporting incidents involving SCI networks to the NSA IC-IRC will be in accordance with IC-IRC CONOPS. In addition to SCI-level reports, NSA IPC also will share appropriately sanitized reports with collateral-level DOD CERT organizations to ensure vulnerabilities reported on compartmented systems are disseminated to administrators of collateral systems.

(7) Organizations at all levels will report changes in the status of events, incidents, and incident-handling actions. Status reports will be issued to the appropriate organizations when:

(a) There are increases, decreases, or changes in the nature of the reportable event or incident activity.

(b) Corrective actions are taken that change the status of the reportable event or incident activity.

(c) A reportable event or incident has been declared closed.

c. Reporting Methods. Table B-B-1 summarizes means in use today in order of preference. Reports should be submitted based upon the most protected means available for the affected system. Use SIPRNET or STU-III if those systems are available. The use of unclassified reporting means (NIPRNET, nonsecure fax) should only be used for incidents on unclassified systems. DOD CERT will work with Service or agency CERTs or CIRTs and combatant command or RNOSCs to correlate and deconflict incident reporting information. The system in which the computer incident took place should not be used, meaning "out of band" reporting should be used if at all possible.

Order	Method	Use
DATA		
1	Integrated Network Management System (INMS) Trouble Management System	For RNOSC and GNOSC use (Future: Service or Agency CERT or CIRT and LCCs with INMS capability)
2	SIPRNET	All levels; combatant command preferred

Table B-B-1. Reporting Methods

Order	Method	Use
3	AUTODIN (Record message traffic)/DMS (AUTODIN Replacement)	All levels; preferred by IC for reliability and security.
4	NIPRNET with security protection (e.g., encryption)	All levels
5	NIPRNET, with no security protection (e.g., encryption)	All levels; least secure method
Fax/Voice		
1	Secure Fax	All levels
2	STU-III/STE	All levels
3	Defense Red Switch Network (DRSN)	All levels
4	Nonsecure Fax	All levels
5	DSN	All levels

Table B-B-1. Reporting Methods (cont'd)

d. Incident Categories

(1) Incidents reported to the DOD CERT shall be categorized according to the framework outlined in Table B-B-2.

Category	Description
<b>0</b>	<b>Exercise or Red Team Activity</b>
<b>1</b>	<b>Root Level Intrusion:</b> An unauthorized person completely controlled (root level) a DOD computer
<b>2</b>	<b>User Level Intrusion:</b> An unauthorized person gained user level privileges on a DOD computer
<b>3</b>	<b>Attempted Access:</b> An unauthorized person specifically targeting a service/ vulnerability on a DOD computer in order to gain unauthorized or increased access/privileges, but is denied access
<b>4</b>	<b>Denial of Service:</b> Use of a DOD computer or computer system is denied due to an overwhelming volume of unauthorized traffic
<b>5</b>	<b>Poor Security Practice:</b> A DOD computer was incorrectly configured or a user did not follow established policy

Table B-B-2. Incident Categories

Category	Description
6	<b>Scan/Probe:</b> Open ports on a DOD computer were scanned with no DOS or mission impact
7	<b>Malicious Logic:</b> Hostile code successfully <b>infected</b> a DOD computer. Unless otherwise directed, only those computers that were infected will be reported as a Category 7 incident.
8	Unknown

Table B-B-2. Incident Categories (cont'd)

(2) Incidents shall be reported in accordance with the standard timeline in Table B-B-3. The reporting timeline is designed to expedite reporting of those Priority 1 incidents (Table B-B-2) where national-level coordination and action may serve to mitigate or prevent damage to the GIG. Additionally, the reporting timeline extends the amount of time available for CND Service Providers to collect, process, and correlate information concerning Priority 2 (Table B-B-2) events before reporting them to the national level. Nothing in this manual shall preclude the rapid reporting of any event deemed necessary by the responsible CND Service Provider.

e. Incident Report Format

(1) The incident report format, Table B-B-4, will be used for an initial report of incidents or reportable events. The following report format provides a structure for reporting initial incidents telephonically, by secure fax, or by other electronic means. Initial reports may be incomplete. Reporting organizations should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

(2) In the initial report, the user will provide as much information as possible. C/S/As may amend the format to require more information for internal uses. As more information becomes available, provide additional detail in follow-on incident reporting.

(3) Incident-handling organizations will provide feedback to reporting organizations as information is developed. Subordinate echelons in the reporting chain are responsible for relaying the information to the originating point and developing procedures to disseminate the information as appropriate within their constituent communities (CERT or CIRT within the Service,



Defense agency, or combatant command and/or RNOSC within their area of responsibility (AOR)).

<b>Category</b>	<b>Reporting Timeline</b>	<b>Method of Reporting</b>
0	Use reporting timelines outlined for Category 1-7 that exercise or red team activity is replicating	Telephone E-mail Approved methods
1	Ongoing: 1 hour from detection. Existing: 24 hours following validation by CND service provider.	Telephone E-mail Approved methods
2	Ongoing: 1 hour from detection. Existing: 24 hours following validation by CND service provider.	Telephone E-mail Approved methods
3	48 hours following validation by CND service provider.	E-mail Approved methods
4	Ongoing: 10 minutes following start of activity. Event in Progress: Follow up report 1 hour after initial report. Additional reports shall be made on a schedule not to exceed 3 hours. Closeout Report: 48 hours after cessation of DOS.	Telephone E-mail Approved methods
5	48 hours following validation by CND service provider.	E-mail Approved methods
6	Major: 10 minutes from detection. Minor/Routine: 24 hours following validation by CND service provider.	Telephone E-mail Approved methods
7	Major (outbreak in progress): 10 minutes after detection. Minor (individual systems infected, no large outbreak): 24 hours following validation by CND service provider.	Telephone E-mail Approved methods
8	Ongoing: 1 hour from detection. Existing: 24 hours following validation by CND service provider.	Telephone E-mail Approved methods

Table B-B-3. Incident Reporting Timelines

25 March 2003

<b>Report Classification:</b>		Organization Incident Tracking Number :	Reporting Organization
<b>From:</b>	Reporting organization (component command, GNOSC/DOD CERT, combatant command)		
<b>To:</b>	Lower echelons will forward to those elements specified by their component command		
<b>Date/Time Incident Occurred</b>	ZULU date time group (DTG) that incident actually occurred.		
<b>Date/Time of Incident Discovery/ Identification</b>	ZULU DTG that incident was discovered (via routine log review, automated alert, system failure, etc).		
<b>Date/Time of Report:</b>	ZULU DTG of report submission.		
<b>Category of Incident: (identify)</b>	Category of incident (e.g., CAT 1-7).		
<b>Source IP/ Intruder</b>	Provide source IP with resolution data identifying owner and country of source IP machine. If the intruder is known, provide all identifying information to include objective of intruder, if known. (Source IP is not necessarily indicative of true origin)		
<b>Target IP</b>	Provide target IP with resolution identifying responsible command and physical location of target IP machine (B/P/C/S, etc)		
<b>Technical Details: (identify)</b>	Provide a narrative description of the incident with technical details. Include DTGs of significant events (start, stop, or change of activity). Identify the OS and version running on target machine. State the use of the targeted system and whether the system is on or off-line. Indicate whether the incident is ongoing.		
<b>Technique/ Exploit Used:</b>	Provide details on specific technique(s), tools, or exploits used, if known.		
<b>Vulnerability:</b>	Identify the vulnerability exploited, if known. Identify IAVA, if any, that applies to the vulnerability and whether the system was thought to be IAVA compliant.		

Table B-B-4. Incident Report Format

<b>Unauthorized Results:</b>	Described what the intruder achieved.	
<b>Mission Impact: (assess)</b>	Provide a narrative description of impact with a brief description of affected systems, networks and information. Mission impact assessment should be classified in accordance with DOD 5200.1-R and DOD Instruction 3600.2.	
<b>Actions Taken: (inform / respond)</b>	Indicate what action has been taken in response to the incident. Include notifications and associated reports.	
<b>Coordination: (inform / respond)</b>	Describe any coordination (give command name) that has been accomplished on this incident)	
<b>Contact Information:</b>	Name:	
	Telephone:	
	Fax:	
	E-mail:	

Table B-B-4. Incident Report Format (cont'd)

(4) For an incident report to be considered “complete” it will contain, at a minimum, the following information.

- (a) Category (level).
- (b) Title – of incident level.
- (c) Mission impact (minimal or significant).
- (d) Reporting CERT.
- (e) Reporting CERT incident number.
- (f) Type of incident (e.g., web defacement).
- (g) Source IP and port.
- (h) Intruder(s) (if known hacker – name or handle).
- (i) Origin (country).
- (j) Target IP(s) and port.

- (k) Service or DOD component.
- (l) Unit or Organization.
- (m) Location (base, camp, post or station).
- (n) Vulnerability.
- (o) Technique, tool or exploit used.
- (p) Date occurred.
- (q) Date identified.
- (r) Date reported.
- (s) Date closed.
- (t) OS and version of OS.
- (u) Applicable IAVA.
- (v) Use of target (e.g., web server or file server).
- (w) Classification.
- (x) DOD Network.
- (y) Synopsis (details of the incident).
- (z) Action taken (e.g., system off line or law enforcement informed).

f. Follow-on Incident Report

(1) The incident report format (Table B-B-4) will be used for all subsequent or follow-on reports. Additional reporting will provide the raw details needed for the regional or global teams to understand the technical nature of the problem and will be merged with information obtained from other reports to highlight regional or global trends. This form will be forwarded by secure E-mail or any of the approved secure reporting methods. For example, record message traffic more readily supports automated intelligence database handling requirements.

(2) The DOD CERT will provide timely feedback to reporting organizations as more information becomes known. Feedback will flow back through the incident reporting structure (Figure B-B-1). Subordinate layers in the reporting channels are responsible for relaying this information to the originating point and developing procedures to disseminate the information as appropriate within their constituent communities (CERTs and/or CIRTs within the Service, agency, or combatant command and/or RNOSC within their AOR). The format is also used by CERTs and/or CIRTs or combatant command and/or RNOSC organizations to report information developed through observation, correlation, analysis, or other means.

g. Protection of Incident Reports. Incident reports will be protected based on their classification and at the sensitivity level of the affected system. All incidents occurring on the SIPRNET shall be classified at least SECRET. Classifying an incident higher than SECRET will depend upon the classification level of the material involved (TOP SECRET, compartmented), overall impact, and compromise potential. Incidents occurring on NIPRNET systems will be unclassified and marked FOR OFFICIAL USE ONLY (FOUO) unless an adversary's exploitation of information in the report would result in classified information compromise or present a significant negative impact on a national security organizational mission. Classified incident reports will be classified and protected in accordance with DOD 5200.1-R (reference i) and DOD Instruction 3600.2 (reference u).

### 3. Vulnerability Analysis

a. The primary purpose of vulnerability analysis is to assess the security posture of automated information systems. Vulnerability analysis may be conducted and requested at different organizational levels, including the system administration level. For instance, a SA may conduct a vulnerability analysis with support from an outside agency. Vulnerability analysis may be undertaken to ensure that automated information systems and security features (auditing software) are properly configured for secure system operations. For security purposes, once inappropriate activity is verified, established incident and vulnerability reporting procedures must be followed. An incident must also be reported to the applicable law enforcement organizations for appropriate action if a violation of law is evident or suspected.

#### b. Protection of Vulnerability Reports

(1) Vulnerability reports for information systems will be classified and protected in accordance with this manual, DOD 5200.1-R (reference i), CJCSI 6510.01C (reference b), and DODI 3600.2 (reference u).

25 March 2003

(2) Vulnerability reports for commercial off-the-shelf (COTS) systems or components (hardware, firmware, or software) will be unclassified and marked FOUO unless an adversary's exploitation of information in the report would result in classified information compromise or a significant negative impact on a national security organizational mission. In those instances, the report will be classified appropriate to the level of classification of information processed on the system or the expected level of harm to national security if the vulnerability were to be exploited.

(3) Reports of vulnerabilities on information systems (to include the operational intelligence and legal sources and methods employed to identify, define, describe, and report incidents and vulnerabilities) not available for purchase by the general public will be marked with the classification upon which the system containing the vulnerability is operating.

(4) The originator of a vulnerability report will determine the classification of the report based on DOD 5200.1-R (reference i) and DODI 3600.2 (reference u).

#### 4. Incident and Vulnerability Feedback Methods

a. The IAVM program implements a comprehensive distribution system for DISA GNOSC (DOD CERT) vulnerability alerts and countermeasure information. See Appendix A of Enclosure B, "Information Assurance Vulnerability Management Program," for more information on the IAVM process.

b. DOD CERT generates a variety of management, technical, and analytical products and maintains an Internet newsgroup on SIPRNET to support real-time dissemination of information during periods of heightened activity. These reports are available on the SIPRNET at <http://www.cert.smil.mil>.

## APPENDIX C TO ENCLOSURE B

## INFORMATION OPERATIONS CONDITION

1. Introduction. This appendix provides a general unclassified description of the DOD INFOCON system. The specific classified guidance and procedures for the reporting process, formats, directive actions, and security can be accessed at the USSTRATCOM West website (<http://www.usspace.spacecom.smil.mil/sj3/sj39/html/index.htm>). The website provides the current coordinated DOD INFOCON system guidance and procedures.

2. Purpose. The INFOCON system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against DOD information systems and networks. The system provides a predefined sequence of actions necessary for achieving a common level of information security for DOD information systems.

3. Applicability. The INFOCON system including responsibilities, processes, and procedures applies to the Joint Chiefs of Staff and all DOD activities within the unified commands, military services, and DOD Agencies.

a. Commander's Alert System. The INFOCON system is executed by unified and Service commanders as well as agency directors with authority over information systems and networks (operational and/or support) and/or operations units (hereby collectively referred to as "commanders"). This alert system is implemented primarily via operations and network centers.

b. Implementation Support. In addition to commanders, effective implementation of the INFOCON system also relies on the mission support community. This function establishes and maintains information systems and networks and the associated services they provide to DOD commanders. The support function also encompasses network security activities and includes, but is not limited to, positions such as the DAA and IAO. The INFOCON system will impact individual DOD users only to the extent necessary to ensure the integrity of DOD computer networks and information systems. This includes vigilance in computer security practices and maintaining situational awareness to report anomalous activity to their respective IAO.

4. Authority

a. Operational. The INFOCON system is established by the Secretary of Defense and executed through the operational authority of the

25 March 2003

CDRUSSTRATCOM as part of his overall responsibility for CND for the Department of Defense.

b. DOD INFOCON Declaration. The Secretary of Defense designated CDRUSSTRATCOM as the DOD INFOCON declaration authority for the Department of Defense.

c. Local INFOCON Declaration. Commanders at all levels of the Department of Defense retain the authority to declare INFOCONs for information systems and networks within their area of command at levels equal to or higher than the DOD level.

## 5. Description

a. Network Defensive Posture System. The DOD INFOCON system is characterized by a set of defensive postures consisting of directed measures implemented uniformly across the Department of Defense. It provides a risk mitigation tool to aid the commander in proactively declaring postures and directing defensive actions based on advanced I&W of hostile activity. The INFOCON system also guides the commander in identifying the INFOCON posture in the event predictive intelligence is not possible. The uniform application of directive, pre-planned measures will promote predictable responses to crises and provide timely, accurate, and clear direction to DOD commanders. Flexibility is built into the INFOCON system to allow additional specific actions to be mandated, based on the threat. Thus the INFOCON system provides a range of defensive measures that support operations at all levels of conflict, from peacetime operations through combat operations and back to restoration of peace.

### b. Scope

(1) The INFOCON system pertains to all DOD information systems and networks operating at the TOP SECRET level (not to include closed, special enclave, or IC networks) and below. The system also governs any interconnections between public and DOD unclassified networks (e.g. Internet to NIPRNET), DOD unclassified to classified networks (e.g. NIPRNET to SIPRNET), and classified to classified networks (e.g. SIPRNET to JWICS).

(2) The IC IRC will serve as the defense IC central reporting and coordination center for CND activities that pertain to closed, special enclave, and/or IC networks. Commanders of closed, special enclave, and/or IC networks may use the INFOCON system as a basis from which to assess and direct similar actions for these networks.



25 March 2003

6. Assumptions. Several critical assumptions were made about the nature of military operations in a hostile information environment in developing the DOD INFOCON system. Understanding these assumptions is essential to effectively implement this system.

a. Self-Imposed Denial of Service. The INFOCON system must support the commander's ability to perform assigned mission critical responsibilities without major operational mission degradation. The implementation of INFOCONs must not impair a commander's capability to conduct operations. The reliance on information systems for critical operational and support functions, such as command and control, intelligence, and logistics means that the Department of Defense cannot afford to disconnect from these critical resources or other units and/or agencies. The Department cannot allow an adversary to drive it into a self-imposed denial of service. The key tenet is that the Department of Defense will stay connected, if possible, while minimizing all non-essential connections.

b. Shared Risk. In today's network-centric environment, risk assumed by one is potentially a risk shared by many. Trust relationships and unresolved vulnerabilities may expose multiple commands and organizations to malicious activity. This necessitates a common understanding of the threat, INFOCON level, and defensive measures implemented with the declared INFOCON. It also requires that a single entity retain the final authority for actions necessary to protect DOD information systems and networks. This authority is assigned to CDRUSSTRATCOM.

c. Insider Threat. An adversary may be assisted by an individual or individuals that possess legitimate authorized and trusted access to DOD networks. The presence of an insider threat represents a significant challenge for CND.

d. Anonymity of Intruder. Attributing the malicious activity to its ultimate source may not occur until well after the malicious activity has been detected, if at all. This limits the range and type of options available to military decision-makers.

7. INFOCON Structure. The INFOCON system is characterized by five defensive postures designed to mitigate risk.

a. INFOCON NORMAL. Routine CND operations and normal readiness of DOD information systems and networks characterize INFOCON NORMAL. There is little risk to ongoing military operations. Information networks are operational. Operational impact of degradation or loss of information and information systems is low. DOD INFOCON Concern Assessment is Low.

25 March 2003

There are wide-scale network probing and/or ambiguous patterns of uncoordinated events, incidents, and intrusions. These activities generally involve routine or non-time essential systems and/or networks.

b. INFOCON ALPHA. Involves increased intelligence watch and strengthened security measures of DOD information systems and networks above that of INFOCON NORMAL. INFOCON ALPHA is a condition of preparatory CND operations with a limited risk to operations. Operational impact of degradation or loss of information and information systems is low to medium.

c. INFOCON BRAVO. Involves a further increase in CND readiness above that required for INFOCON ALPHA. Risk to mission accomplishment is moderate, requiring increased network defense and vigilance to maintain network security.

d. INFOCON CHARLIE. Involves a further increase in CND readiness above that of INFOCON BRAVO. INFOCON CHARLIE is characterized by concentrated CND operations capable of functioning in a prolonged threat environment. Risk of mission failure is high and operational impact of degradation or loss of information and information systems is medium to high.

e. INFOCON DELTA. This level is the maximum CND readiness. INFOCON DELTA is a condition of critical CND operations in which the total IO resources of the declaring commander are employed. The risk to mission operations is extreme and the operational impact of degradation or loss of information and information systems is high.

8. Support. Questions concerning DOD INFOCON procedures and processes should be addressed to Computer Network Operations, SP/J39I, commercial phone 719-556-8701, DSN 834-Ext.; Unclassified FAX: 719-556-8886; Secure FAX: 719-556-8885.

25 March 2003

## APPENDIX D TO ENCLOSURE B

JOINT INFORMATION ASSURANCE  
RED TEAM OPERATIONS

1. Purpose. To establish basic steps, responsibilities, and procedures for IA Red Team operations against information systems and networks.

2. General

a. IO is becoming an increasingly important factor in every element of national power, as well as a source of vulnerability. IO, both offensive and defensive, allows the joint force to attain a relative advantage in the information environment. This in turn will significantly complement traditional forms of military activity and is crucial to our success in addressing the growing challenge of asymmetric warfare. The joint force draws upon many activities in the conduct of IO and of information warfare (IW) during crisis and conflict.

b. IA Red Teaming is an essential gauge of CND operational readiness or components and the networks that sustain their operations. This independent and threat-based activity simulates an opposing force and is focused on improving readiness. Red Team support is available from NSA and may be available at the DOD component level. There are three phases of evaluation provided by NSA:

(1) Phase I - A vulnerability assessment team (VAT) for baseline review of defense posture on networks, user workstations and organization IA policy.

(2) Phase II - the Blue Team performs friendly assist once vulnerabilities are identified by the VAT. Blue Team provides key guidance on increased areas of concern in order to quickly remedy and strengthen deficient policy and procedures implemented at the organization.

(3) Phase III - The Red Team deploys to emulate the capabilities and methods of an adversarial force targeting DOD information systems, including developmental systems. Red Teams gather target system(s) knowledge, approximate the adversary target threat environment, gather appropriate attack tools, and train to effect the attack. The Red Team then deploys and launches the assault, documenting the vulnerabilities and suggesting countermeasures. Red Teams work closely with system owners demonstrating how the attacks were run and how owners can protect their systems. Red Teams provide an accurate assessment on which system owners and

25 March 2003

developers can make coherent risk-management decisions concerning their information systems, networks, and supporting infrastructure.

c. The use by the opposing force of other activities and capabilities such as electronic warfare (EW), psychological operations (PSYOP), military deception, physical destruction, and other military capabilities will not be addressed in this appendix. These activities and capabilities should be addressed in the planning and execution of larger exercises.

d. Red Team assessment activities can be broadly separated into certain categories.

(1) Exercise-related activities to provide IA and CND training to the joint force, people, operations, and tools that operate and protect US information systems and networks. This training ensures CND mission processes, procedures, and vital DOD and/or component-wide coordination and actions are realistically implemented. Commanders and agency directors must determine Red Team objectives prior to the exercise or training event. Training and exercises can be conducted at three levels.

(a) Level 1, Computer Network Defense Awareness. The objective of the training event or exercise is to “educate” the people (commanders, staff members, SAs, IAMs, IAOs) or the organizations (headquarters, CERTs and/or CIRTs), NOSCs, etc.). At this level, the Red Team activities would be announced beforehand to facilitate a training environment. This is to allow people and organizations to observe techniques and tools and walk through the processes and procedures to counter the threat.

(b) Level 2, Exercise. The objective of the training event or exercise is to “exercise” the people and organizations in a more realistic environment. At this level, the activities would be announced, possibly as part of a larger exercise. However, the exercise participants would not know exact techniques employed or timing within the exercise. For example, exercise events in the buildup to the exercise or during the exercise may provide information and/or intelligence that indicates an increased threat level, which in turn might indicate a need to increase readiness (e.g., INFOCON change).

(c) Level 3, No Notice Exercise. The objective of the training event or exercise is to provide the “most realism possible” within safety constraints. At this level, the Red Team activities would be unannounced and may or may not be part of a larger exercise. This is the “run” phase of exercising people and organizations on their ability to protect and defend their information systems and networks.

(2) Conducting network-penetration testing (external or internal to the network) to identify vulnerabilities within organization information systems or networks.

(a) This activity by the Red Team can either be announced or unannounced.

(b) The request may be from an organization itself or from a higher headquarters or JTF commander.

(c) The purpose is not training, but to help organizations identify and fix vulnerabilities within their information systems and networks.

### 3. Considerations and Guidelines for IA Red Team Operations

a. Requesting Red Team Support. A commander or agency director of an organization may request support of an IA Red Team.

(1) The requesting authority (commander or agency director) must have ownership or authority over the facilities or systems to be targeted by the Red Team. Note: Commanders and agency directors need to consider requests for Red Team support early in planning due to the limited number of Red Teams and applicable resources.

(2) In most circumstances, the exercise WHITE CELL is also the controlling authority responsible for overall IA Red Team activity for any specific Red Team operation (i.e., exercise support or network-penetration testing).

(3) The requesting authority determines:

(a) Purpose of Red Team operations (i.e., exercise support or network-penetration testing).

(b) Targets for Red Team (i.e., which information systems and/or networks), safety guidelines, and restraints or constraints on Red Team operations. Depending upon the Service level and purpose of the Red Team engagement, constraints should be kept to a minimum to ensure a realistic environment.

(4) The requesting authority also ensures the formation of a control element (White Team), responsible for planning, monitoring, and controlling the exercise. They will collect metric data and adjudicate local disputes. The control element also provides containment and termination authority.

b. Red Team

(1) C/S/As are authorized to form Red Teams to support exercises, training, and network-penetration testing to support IA Red Team operations. The C/S/A will:

(a) Ensure IA Red Team operations are planned and executed in compliance with this manual, to include appropriate legal review by C/S/A legal or general counsel.

(b) Designate an office of primary responsibility (OPR) for C/S/A Red Team operations.

(c) Ensure IA Red Team OPRs coordinate all associated CNA and CNE activities with the JTF-CNO and USSTRATCOM, so they are situationally aware of all Red Team activities.

(d) Ensure all IA Red Team operations are coordinated with NSA and IA Red Team OPRs of affected DOD components.

(e) Ensure that non-attributable Red Team lessons learned are incorporated into the Joint Universal Lessons-Learned System (JULLS) database.

(2) DIRNSA has developed and maintains an IA Red Team capability. This team may be requested for employment in joint and national-level exercises.

(3) C/S/As will ensure that personnel who conduct IA Red Team operations are trained and certified in the proper application of IA Red Team tools, techniques, and procedures, and possess requisite security clearances commensurate to the level of classification of the data or information systems they will be operating within or against. At a minimum, such personnel must be cleared to:

(a) The security level of data against which they are conducting Red Team operations.

(b) The security level of the tools or techniques employed in the performance of IA Red Team operations. Note that higher clearances may still be required.

(4) Red Team members should always be aware during exercises and training events that the goal is to provide realistic and useful training opportunities and lessons learned to the participants. The purpose of network-penetration testing operations is to identify vulnerabilities to assist organizations in taking corrective action.

c. Identifying the Objective(s)

(1) Are the objectives intended to test people, processes, information systems, networks, technologies, or operations?

(2) Are the objectives intended to obtain access to a certain type or classification level of information?

(3) When Red Team activities are part of a larger exercise, planners must ensure that Red Team objectives mesh with exercise objectives. Coordination and integration of planning Red Team operations into an exercise must ideally occur in the initial planning stages.

d. Threat Portrayal. The goal is an independent and threat-based (postulated and/or known) force, which is employed to improve the readiness and defensive IA readiness and CND operations of joint and DOD components. An IA Red Team is an interdisciplinary, simulated opposing force that utilizes active and passive as well as technical and nontechnical capabilities on a formal, time-bound tasking to expose and exploit vulnerabilities of friendly information systems. Employment considerations include:

(1) What threat will the Red Team portray (e.g., script kiddies, hackers for hire, crackers, terrorists, nation state, turned insider, unwitting insider)? The threat level identified should appropriately match the exercise objectives. For example, one of the objectives may be to practice coordination and procedures to detect, track down, and respond to an individual and/or group conducting attacks against the Department of Defense. Due to the exercise time constraints, a highly skilled, nation-state level threat would not meet these exercise objectives because of the stealthy nature in which they operate.

(2) What type of information capabilities will be used?

(3) What would the threat's objectives be in the given scenario, and how would those capabilities be used against the joint force?

e. Safety

(1) Safety in IA Red Team operations is a primary concern.

25 March 2003

(a) A controller or neutral (white) team, appropriately staffed, will be employed in all IA Red Team operations and will be thoroughly integrated with adversary (red) and friendly (blue) teams to ensure control and safety of operations.

(b) An appropriately staffed and cognizant trusted agent network (e.g., CERT and RCERT) will be employed to assist in higher planning, control, or evaluation of IA Red Team operations.

(c) The controller or White Team will be the primary organization responsible for safety and security of IA Red Team operations. The White Team and the Red Team will have the authority to initiate a "stop exercise" order if safety parameters established by the requesting authority are exceeded and pose a risk to personnel or infrastructures or in the event of real-world operations.

(2) Joint Red Team operations will not intentionally damage or permanently degrade facilities or systems being targeted, unless directed to do so by the system owner.

(a) This includes systems the IA Red Team may utilize to gain access to the targets (including commercial Internet Service Providers (ISPs)).

(b) The requesting commander or agency director and the commander or chief of IA Red Team will be apprised of any risk of damage or degradation associated with Red Team activity prior to the commencement of operations.

(c) Upon completion of IA Red Team operations, the target facility or system will be restored to the same operating condition as it was prior to the initiation of Red Team operations, unless the facility or system has been declared off-limits and/or taken off-line.

f. Legal Considerations

(1) The C/S/A staff judge advocate or legal and/or general counsel will provide legal oversight and guidance for DOD IA Red Team operations to the requesting commander or agency director.

(2) IA Red Team operations will conform to all applicable US laws and those treaties and protocols to which the United States is a signatory.



25 March 2003

(3) All Red Team operations will employ procedures and safeguards to ensure compliance with these applicable laws, treaties, and protocols.

(4) Particular attention will be paid to safeguard the privacy of US citizens.

(5) Suspicion of unlawful activity discovered in the course of IA Red Team activities will be immediately reported to the appropriate staff judge advocate or legal and/or general counsel. Normally, affected Red Team activities will cease upon discovery of unlawful activity and will not resume until appropriate measures have been initiated and official authorization to resume is granted.

g. Non-DOD Systems

(1) Organizations conducting Red Team activities will develop appropriate procedures and safeguards to ensure their efforts do not affect non-DOD systems.

(2) Authority to access non-DOD facilities or systems may require agreements and/or approvals requiring legal review. IA Red Team operations that utilize commercial ISPs will comply with DODD 5105.61 (reference v) or seek a waiver from the appropriate component general counsel.

h. Use of a Trusted Agent Network

(1) The DOD trusted agent network consists of all trusted agents within the Department of Defense. This network has been established by NSA in coordination with USSTRATCOM, DISA, the Services, and other combatant commands and agencies.

(2) The purpose of the trusted agent network is to provide a representative group of trusted insiders. They are to keep each C/S/A informed of all ongoing IA Red Team activities. A trusted agent may be a member of a CERT.

(a) The trusted agent ensures exercise safety and assists in deconflicting exercise play from real-world activity.

(b) Trusted agents are informed of all ongoing joint IA Red Team operations so they may assist in deconflicting as required.

(3) Direct supervisors and exercise coordinators will be made aware of the overall trusted agent program and their responsibilities to ensure

deconfliction of exercise play from real-world activity. Trusted agents will not be forced to reveal specific information “entrusted” by a Red Team such as when active operations are beginning or ending.

i. Protection of Vulnerability Information

(1) The identification and correlation of vulnerabilities to individual facilities, systems, networks, or critical infrastructures is a sensitive matter that could place the DOD mission at risk.

(2) Documentation and reporting of vulnerabilities will be classified in accordance with DODI 3600.2 (reference u) and other appropriate plans, operations, or program security classification guides.

j. Security of Red Team Capabilities

(1) Appropriate security measures will be employed by the IA Red Team.

(2) Attack capabilities will not be used without prior concurrence of the requesting authority.

(3) Special access controls required to protect IA Red Team capabilities or results of IA Red Team operations will be applied in accordance with applicable Service or agency directives as required.

k. Lessons Learned

(1) A formal report will be provided to the requesting commander or agency director identifying vulnerabilities (and those that require immediate attention) revealed during IA Red Team operations.

(2) Specific IA Red Team report results will not be disseminated without the requesting commander's or agency director's prior approval.

(3) IA Red Team lessons learned will be sanitized to eliminate possible attribution and incorporated into the JULLS database.

l. Intelligence and Counter-Intelligence Support

(1) Joint IA Red Team operations will incorporate real-threat intelligence whenever possible to provide for a realistic opposing force.

25 March 2003

(2) Joint IA Red Team operations will incorporate intelligence and counterintelligence scenarios whenever possible to produce a complete assessment of a facility's vulnerability to attacks on its information infrastructure.

4. Support. For NSA Red Team Support, contact either the NSA Military Customer Advocate Office (V15) 410-854-4711 (DSN 244) or NSA Information Assurance Red Team, Planning Branch (X62) 410-854-7901.

(INTENTIONALLY BLANK)

APPENDIX E TO ENCLOSURE B  
IA INTEGRATION INTO JOINT PLANS AND PLANNING  
TO BE PUBLISHED

(INTENTIONALLY BLANK)

## ENCLOSURE C

## DEFENSE-IN-DEPTH – DEFENDING THE INFORMATION ENVIRONMENT

1. Defense-in-Depth

a. This enclosure focuses on the four defense-in-depth areas:

- (1) Defending the computing environment.
- (2) Defending the network.
- (3) Defending the enclave boundary.
- (4) Supporting infrastructures.

b. This enclosure provides basic background on the four defense-in-depth areas, the objectives, and basic security requirements that should be implemented.

c. The individual appendices in this enclosure focus on particular areas important to developing a defense-in-depth strategy.

d. DODI 8500.2 (reference w) provides baseline IA controls established by mission category and security classification.

2. Defending the Computing Environment

a. Defending the computing environment is focused on servers; workstations; the applications installed on them; and the supporting services, such as host-based intrusion detection, necessary for network operations. An application is any software written to run on a designated OS.

(1) Figure C-1 depicts a high-level view of defending the computing environment.

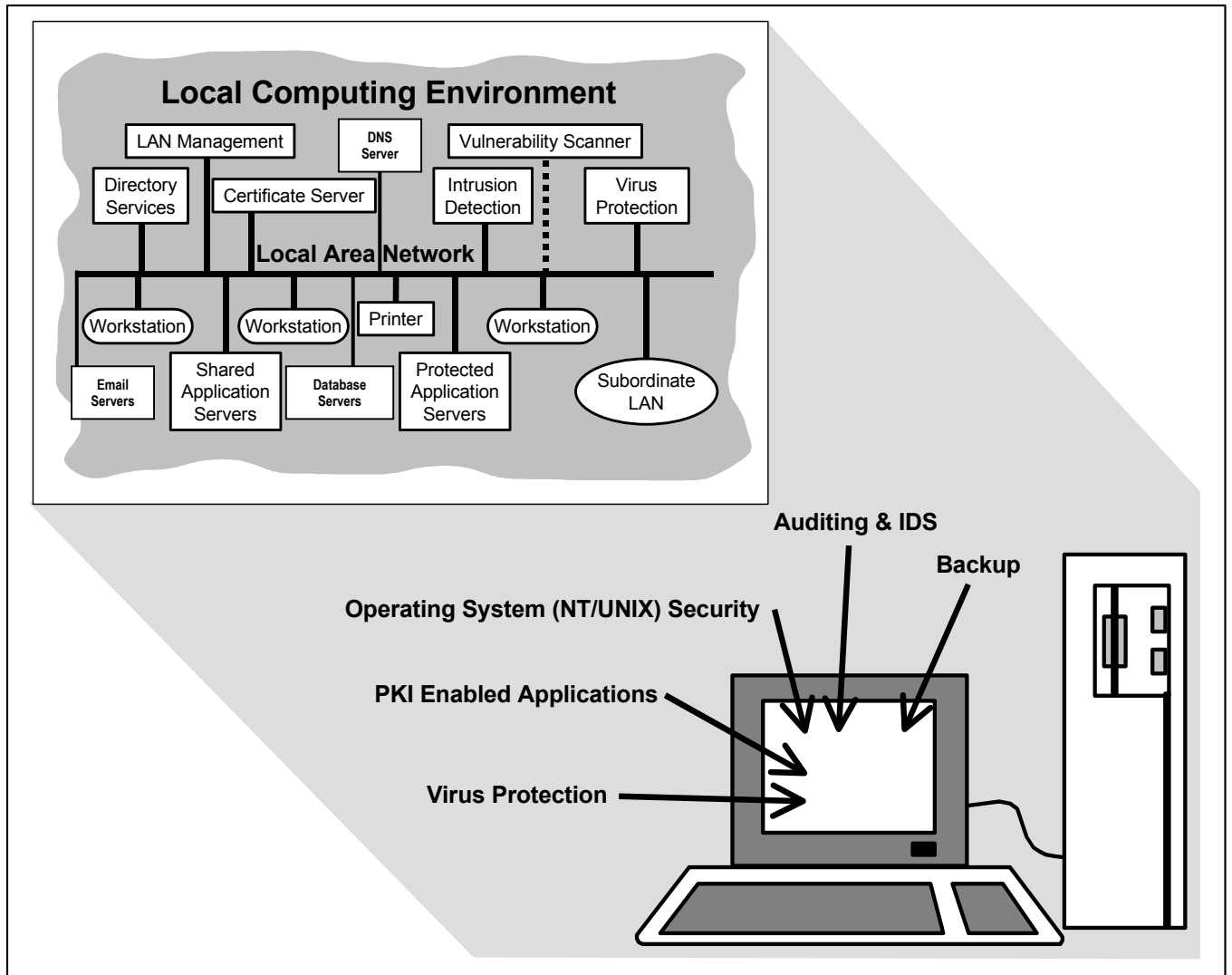


Figure C-1. Computing Environment

(2) Each computing environment (user workstation, server, system and/or subsystem) within the enclave requires a minimum of basic protection.

(3) The computing environment includes the end-user workstation, peripheral devices, servers; and software applications such as word processing, E-mail, web, access control, host-based intrusion detection, and the OS.

b. Defending the Computing Environment Objectives

(1) Ensure that hosts and applications support availability by defending against denial of service.



(2) Ensure the confidentiality and integrity of data processed by the host or application, by preventing unauthorized disclosure or modification of data.

(3) Defend against the unauthorized use of a host or application.

(4) Ensure security tools and features are capable so a variety of applications can be readily integrated with no reduction in security (e.g., to meet the needs of a joint task force).

(5) Maintain configuration management of all hosts to track all patches and system configuration changes.

(6) Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external.

c. Security Requirements. To accomplish the computing environment objectives, the following application security requirements shall be implemented on the system or application:

(1) System-Provided Security Requirements

(a) Maintain system integrity.

(b) Employ physical hardware protection to include maintaining specified environmental conditions for system components.

(c) Conduct basic OS security.

(d) Conduct routine backup and recovery procedures.

(e) Use recommended anti-virus software to protect against viruses, worms, and other malicious software.

(f) Employ host-based intrusion detection software.

(g) Employ physical protections including the protection of media containing application software and application data while not stored on-line.

(h) Implement appropriate procedural security (to include protection, detection, restoration, and recovery).

(i) Ensure all legacy systems are level 5 defense information infrastructure (DII) common operating environment (COE)-compliant. Level 5

compliance provides a minimal DII compliance that ensures applications are interoperable, have the same look and feel, and are segmented using COE installation tools. All new command, control, communications, computers, and intelligence emerging systems and upgrades will be level 6 DII COE-compliant with the goal of achieving level 7.

(j) Conduct identification and authentication of user and system administrator to the computing environment. Ensure individual accountability through automated or administrative means.

(k) Conduct routine auditing of the information system. Applications need to check user input for malicious code.

(2) Application Provided Security Requirements

(a) Ensure user information confidentiality as it passes from the originator via the server(s) to the recipient(s).

(b) Ensure keying material information confidentiality.

(c) Ensure originator and recipient confidentiality.

(d) Protect application software's integrity during distribution.

(e) Ensure integrity of key material, source and destination information, and any other control information.

(f) Conduct authentication of users and administrators, and system authentication of clients and servers.

(g) Employ application access control (e.g., access control on the mail server).

(h) Conduct auditing and monitoring of the user, administrator, client, and server. Specifically, the system should track all modifications of executable code or data by systems and users as well as system access attempts, both successful and unsuccessful. In addition, provide role-based access control whereby systems and applications should not allow administrators to perform root administrative functions while logged in as a nonroot user.

(i) Nonrepudiation capability is desired and may be required.

(j) Conduct key and information recovery.

d. Technology to Defend the Local Computing Environment. The IA challenge is to provide selected mechanisms (such as protected distribution systems) for protection. In addition to procedures and processes, effective tools must be used to increase the number of defensive layers used to protect end-systems, capabilities, internal components, and associated peripheral devices. Technologies used for this purpose include:

- (1) Passwords, personal identification numbers (PINs), tokens, and biometrics.
- (2) Encryption.
- (3) Digital signatures.
- (4) System monitoring and management tools.
- (5) Intrusion detection tools.
- (6) Malicious code and virus detectors.
- (7) Backup technologies.
- (8) Software with its own access control features.

### 3. Defending the Network

a. Networks and their supporting infrastructures include large transport networks and other transmission and switching capabilities. They may be metropolitan area networks, campus area networks, and wide area networks (WANs) or LANs extending coverage from broad communities to local bases. Figure C-2 depicts a high-level view of defense of the network with suggested placement for IA components and mechanisms. The target environment for network defense includes data, voice, wireless (e.g., cellular, paging), and tactical networks that support both the operational and strategic DOD missions. These networks can be DOD-owned and operated (both service and transport) or leased services (transport layer).

25 March 2003

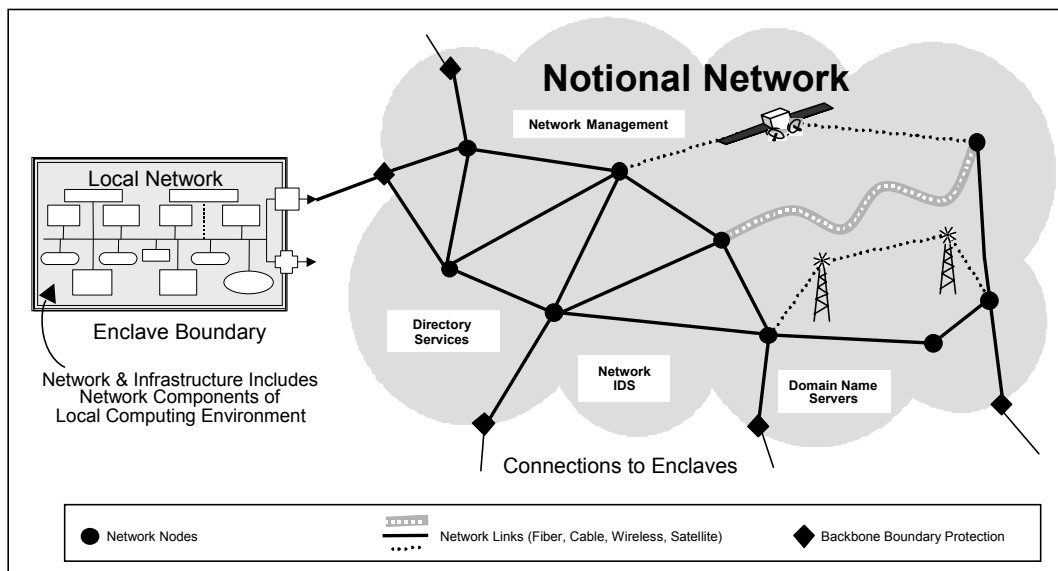


Figure C-2. Defending the Network and Infrastructure

(1) The network layer consists of three distinct types of traffic:

- (a) User Traffic. Information users transmit over the network.
- (b) Control Traffic. Information transferred between network components used to establish user connections.
- (c) Management Traffic. Information that configures network components or network component status information.

(2) The focus of network defense is on the backbone network. The most common examples of a commercial backbone network are the terrestrial-based voice systems and the Internet. In the Department of Defense, the most common data backbone network is the DISN. In discussing security requirements, this enclosure includes wireless systems, satellite systems, and copper and fiber-based terrestrial systems that carry information to include data, video teleconferencing, and voice systems.

b. Technology to Defend Networks. Redundant and multiple data transport paths offer more than one available alternate physical medium or route. These measures serve to ensure continued connectivity when intermediate enclaves or network components are degraded or inoperable. In a crisis enclaves should be able to logically disconnect from external networks by filtering possible malicious traffic at the router or firewall. Contingency planning against denial of service should be included in agreements with commercial services' providers, such as provisions for switching to an alternate

communications path or another provider to avoid a single point of failure. In addition, automated system monitoring and management tools should be used to collect and analyze abnormal phenomena and maintain system status. At a minimum, these tools should be able to detect system disruption and degradation indicative of malicious activity.

c. Defending the Network Objectives

(1) Ensure that DOD systems and networks follow a consistent architecture that is consistent with the joint technical architecture and GIG IA architecture.

(2) Ensure that all DOD enterprise data is protected in accordance with its classification and mission criticality.

(3) Ensure the confidentiality and integrity of the data transmitted by user, control, and management.

(4) Ensure that mission-critical and mission-support networks receive maximum protection against denial of service.

(5) Ensure that networks are visible for IA management and monitoring purposes.

(6) Enhance availability by providing the ability to protect from, react to, and restore operations after a catastrophic event, such as a natural disaster, intrusion, or malicious code attack. This includes developing and exercising contingency plans.

(7) Ensure infrastructure management does not conflict with other backbone or enterprise networks or systems.

d. Potential Threats to the Network

(1) One primary threat is foreign IO. Supported by intelligence exploitation, foreign IO threats include CNA, CNE, EW, radio frequency (RF) weapons, PSYOP, and denial and deception (D&D). Another primary threat is the physical destruction of the information infrastructure or facilities that house network components. The goal is to disrupt, deny, and/or delay the network's mission to move information to warfighters, policy makers, and support personnel. Sources of attacks are global in scope and include potentially hostile, rogue, allied, and neutral state and nonstate-sponsored entities. Additionally, terrorists and insurgents, organized crime, industrial

25 March 2003

espionage, hackers and hacker groups and insiders can also be sources of attack against DOD networks.

(2) Foreign intelligence exploitation (e.g., CNE or human intelligence) of networks can occur through various sources through the Internet, NIPRNET, official unclassified correspondence, and personnel. A vulnerability assessment team can assess the value of unclassified information to a potential adversary. Technical collection (data theft) and analysis capabilities may provide adequate pre-attack information, such as data-flow analysis and network architectural details. Technical collection tools are widely available and increasingly user friendly. DOD systems are regularly probed and scanned in order to define network architecture and assess vulnerabilities via compromised domestic or foreign systems.

(3) CNA can be used against the entire computer network architecture, OSs, software applications, and information. CNA includes inserting malicious code, communications disruption, DOS, and data corruption, modification, and manipulation. The well-publicized distributed DOS attacks against several US-based commercial websites have sensitized foreign countries to their own systems vulnerabilities. Evidence suggests that some foreign entities have used DOS tactics against and introduced malicious code into US information systems. DOS tactics flood networks by consuming bandwidth; they "bury" the network with meaningless communications beyond network capability so that useful bandwidth loss occurs. Other tactics can disrupt network management communications. The intent of these attacks is to interfere with the information flow across the network by attacking the control commands causing service disruptions.

(4) EW tactics can be used against the network's wireless segments. Few commercial products provide electronic protection (EP) technology to defend against electronic attack (EA) and electronic support tactics. The rapid global growth of commercial wireless communications systems has motivated some countries to develop EW tactics against those systems, but not necessarily against the United States. However, foreign IO may impact similar US systems. The trend for DOD networks to increasingly integrate commercial systems can make these nodes potentially vulnerable, especially when a foreign country deploys known EW tactics against them.

(5) RF weapons, such as electromagnetic pulse and directed energy weapons, can be used to physically disrupt electronic circuits. Foreign interest in protecting their own systems against these weapons leads to increased understanding of the capabilities of RF weapons.

(6) PSYOP and D&D may be used against network personnel and facilities.

(7) A more detailed discussion of the foreign IO threat to DOD networks may be found in "The Information Operations Threat to the Defense Information Systems Network (DISN)," DI-2710-6-01 (reference x) available on SIPRNET at [http://delphi-s.dia.smil.mil/intel/world\\_wide/dir/DI-2710-6-01/2710-6\\_cov.html](http://delphi-s.dia.smil.mil/intel/world_wide/dir/DI-2710-6-01/2710-6_cov.html).

(8) Threats to network availability can be grouped into three general threat categories:

(a) Attacks that cause loss of available bandwidth by consuming network bandwidth, preventing legitimate network users from exchanging information.

1. Jamming is usually the easiest to detect and possibly the hardest to counter for a network backbone. Two examples of jamming include jamming between a satellite and a ground station and jamming between cells of a wireless network.

2. Flooding that consumes network bandwidth by "burying" the network with processing communications in excess of network capability is another way that bandwidth loss can occur. Examples include:

a. Problems with telephone systems over holidays or during disasters where everyone tries to use the limited resources at the same time.

b. Active computer flooding using spurious communications traffic.

3. Thefts of service by attackers posing as legitimate users, establishing a connection and using the network to transfer their information. These attacks are very subtle and difficult to detect, as they appear to be normal operations most of the time.

(b) Network management communications disruption interferes network information flow by attacking control commands to the infrastructure devices. Network managers are still able to control the network, but the network is receiving misinformation causing a possible disruption in service. Attacks in this category are specific to the backbone network and how it establishes and maintains the communications pathways to transfer a user's data. In contrast, bandwidth availability attacks impact normal network

operations by consuming processing capability, limiting network availability, not by attacking the infrastructure's devices controlling system.

(c) Attacks against data are intended to either surreptitiously or overtly alter or destroy data contained within the network.

e. Root-Access Controls Security Requirements

(1) Strict control of network devices with root access must be maintained, limited to those with a specified requirement and further delimited to specific areas within those requirements (e.g., a system administrator responsible for a small network within a larger network only requires access to the specific area and/or subsystem for which they are responsible, not the entire network).

(2) Separate user and network administrator accounts and/or passwords must be used.

(3) Critical network functions, such as configuration management and systems maintenance, should be physically separated from noncritical functions such as general E-mail and web surfing.

(4) An audit trail of all root access, as well as all actions performed as roots, should be collected where possible.

f. Device, Database, and Application Control Security Requirements

(1) Network Device Access Control

(a) All network management traffic should originate within the network. Boundary devices should screen traffic at firewall and/or router to ensure that network management traffic does not enter the network from the outside.

(b) Network management requests must be strictly authenticated prior to granting device access or setting up protected channels.

(c) Cryptographically authenticated encrypted communications must be employed to protect dial-up connections, authenticate the identity of the remote operator, and protect the integrity of transmitted data.

(2) Application and database access control. Access to applications will be restricted to authorized users. Automated access control of all databases is required to ensure data integrity.



(a) E-mail Systems

1. Authorized, unclassified government business will use USG E-mail accounts.

2. Contractors and foreign nationals will be identified in their DOD user E-mail address (john.smith.ctr@army.mil or john.smith.uk@army.mil) and electronic signatures (e.g., John Smith, Contractor, J-6K, Joint Staff). Abbreviation used for a contractor in an E-mail address should be "ctr." For additional guidance on foreign nationals and use of country codes, see Appendix B, Enclosure C, "Foreign Access to DOD Information and Information Systems."

3. Unapproved accounts, such as AOL, HOTMAIL or YAHOO, will not be used for official business unless specifically authorized to do so by the DAA. ISP or web-based E-mail systems will be approved only when mission-essential and USG-owned E-mail systems are not available.

4. All mail connections to and from mail servers used for anonymous mail redirection are to be blocked. Mail should be traceable to an individual and to known servers.

(b) E-mail Database Applications. Consistent with security policy, security technologies within the database itself (e.g., password policy, auditing, discretionary access control) will be implemented.

g. Encryption Security Requirements

(1) NSA-approved, high-robustness encryption will be used for all classified traffic that is transmitted across unsecured channels. (See Appendix H to Enclosure C, "Protection Mechanisms – Levels of Concern and Robustness.")

(2) NSA-approved, high-robustness encryption will be used for tunneling SECRET and TOP SECRET data over networks that have a lower classification or releasability restrictions.

(a) NSA-approved, type 1, enclave-based tunneling mechanism is required to tunnel higher classification information over a lower classified network. The mechanism should be under the control of the higher-classification network.

25 March 2003

(b) NSA-approved, type 1 encryption system will be used to tunnel lower classification information over a classified system high or allied and/or coalition network.

(3) Medium-robustness encryption will be used for tunneling sensitive data over unclassified networks.

(4) Commercial solutions may be used that are certified and accredited by the cognizant DAA in accordance with the DITSCAP.

(5) Solutions will be in accordance with the NSA protection profile for tunneling sensitive unclassified data over unclassified networks. More information is located on the Information Assurance Technical Framework (IATF) Forum website ([www.iatf.net](http://www.iatf.net)).

#### h. Data Integrity Security Requirements

(1) Standardized transmission check sums must be employed throughout the network to ensure data integrity.

(2) In case of an incident or catastrophic failure, routine data backup will be used to help ensure data integrity.

#### i. Authentication Security Requirements

(1) Network anti-spoofing capability must be employed to preclude unauthorized use of legitimate identification and authentication data (e.g., impersonating, masquerading, piggybacking, and mimicking are forms of spoofing).

(2) Password (log-on, screen saver) guidance and automated control are required to be used at all times. Passwords must be at least eight characters long and consist of a mix of uppercase letters, lowercase letters, numbers, and special characters, using three of four character sets. Vendor-selected default passwords must be changed during or immediately after system installation. Null or blank passwords are not authorized under any circumstances.

(3) Use of remote access for changing passwords must be severely restricted, unless a strongly encrypted virtual private network (VPN) protects the entire session. System administrators must maintain a complete list of all personnel, devices, and locations authorized to change passwords remotely. Remote change of device maintenance port passwords should be disallowed.

(4) Initially unencrypted passwords should not be transmitted over any network. It is especially critical for system administrator and device maintenance port passwords. Passwords for web applications may normally be changed by the user, but the logon and password management screens must be encrypted with 128-bit secure sockets layer. Forgotten passwords should not E-mailed to the user.

(5) The number of accounts with administrator and/or root privileges, and the number of people having these accounts' passwords, must be kept to a minimum. Following periods of intensive system installation, maintenance and testing, during which many people may require increased access, remove privileges from users' accounts and change passwords on administrator accounts to prevent damage and unauthorized changes to system.

j. Software Security Requirements

(1) Closeout of Factory Defaults. All default accounts and passwords must be changed to prevent unauthorized use. Accounts should be deleted or renamed where possible. Passwords will be changed on all accounts.

(2) Security Configuration Management. C/S/As must have the capability to track software upgrades and must have a process to be notified if these upgrades contain defaults (e.g., back doors) that can be exploited. If defaults exist, then organizations must have the capability to close them and track progress.

(3) Software Patch Status and IAVA Compliance. An automated system is required that can immediately display and report IAVA compliance status. This system must be capable of tracking and recording the software changes (upgrades, etc.) and their impact on previous IAVA-identified vulnerabilities. Patches must be obtained through DOD authorized channels.

(4) Use of automated tools is encouraged to monitor systems performance, audit systems status, and map networks to identify external connections (e.g., possible back doors). SAs will employ automated security tools to monitor password compliance, identify and report IAVA compliance, update antiviral software, and provide a mechanism for IAMs to conduct security certification testing of the systems security features.

k. Networks Security Requirements

(1) Differentiation of User vs. Network Control and Management Data. Network administrative personnel must be able to differentiate between the different types of traffic to afford each the appropriate security.

25 March 2003

(2) Differentiation of Network Usage by Mission Criticality. Networks and networked information must be categorized according to the criticality definitions found in the Information Assurance Guidance and Policy Memo (reference x) to both protect them and perform operational planning for restoration priorities, etc.

1. Virtual Private Network Security Requirements

(1) A standard VPN configuration by an organization is required for effective security.

(2) Authentication certificates and digital signatures must be employed.

(3) Interconnects security requirements are as follows:

(a) Information must be protected to ensure information with a higher classification cannot be moved from a system high network to one operating at a lower security level. Prior to connecting systems of different classifications for transfer of information from high to low, all systems must go through the GIG interconnection approval process (GIAP) (<http://giap.disa.smil.mil>), the Secret and Below Interoperability (SABI), and/or the TOP Secret and Below Interoperability (TSABI) process, as applicable. DISN DAAs must grant approval of the high-assurance guard connecting two or more systems. The SIPRNET Connection Approval Office (SCAO) ([scai@ncr.disa.mil](mailto:scai@ncr.disa.mil) or [scao@ncr.disa.smil.mil](mailto:scao@ncr.disa.smil.mil)) serves as the single POC for SIPRNET connections. Security procedures must include reliable human review.

(b) Interconnects must employ up-to-date antiviral or other malicious-code detection software to identify and remove malicious code when exchanging information between networks.

(c) Interconnects technical solutions must be formally put through the applicable SABI or TSABI approval process prior to implementation.

(4) Bandwidth security requirements dictate that adequate bandwidth allocation for tunneling network control and management information must be reserved. This includes supporting a preemption capability, which allows specified users the right to specific bandwidth regardless of other demands on the system, or to limit the bandwidth available through any access point onto the network.

#### 4. Defending the Enclave Boundary

a. An enclave is an environment under the control of a single authority with personnel and physical security measures. An enclave boundary exists at the point of connection for a LAN or similar network to the service layer. Figure C-3 depicts a high-level view of the enclave boundary with suggested placement of IA components and mechanisms (e.g., firewalls and guards). Enclave boundary target environments include service layer networks, including modem connections; classified LANs within classified WANs (e.g., tunneling information through the SIPRNET); use of virtual private networks on service layer providers; remote enclaves, including remote LANs or systems; and laptops that may be connected remotely to different service networks (e.g., JTF deployments, high-to-low transfer, and low-to-high transfer).

(1) Boundary Definition. The enclave boundary may include multiple LANs, with computing resource components such as servers, routers, firewalls, IDSs, vulnerability scanners, and antiviral and malicious-code detectors.

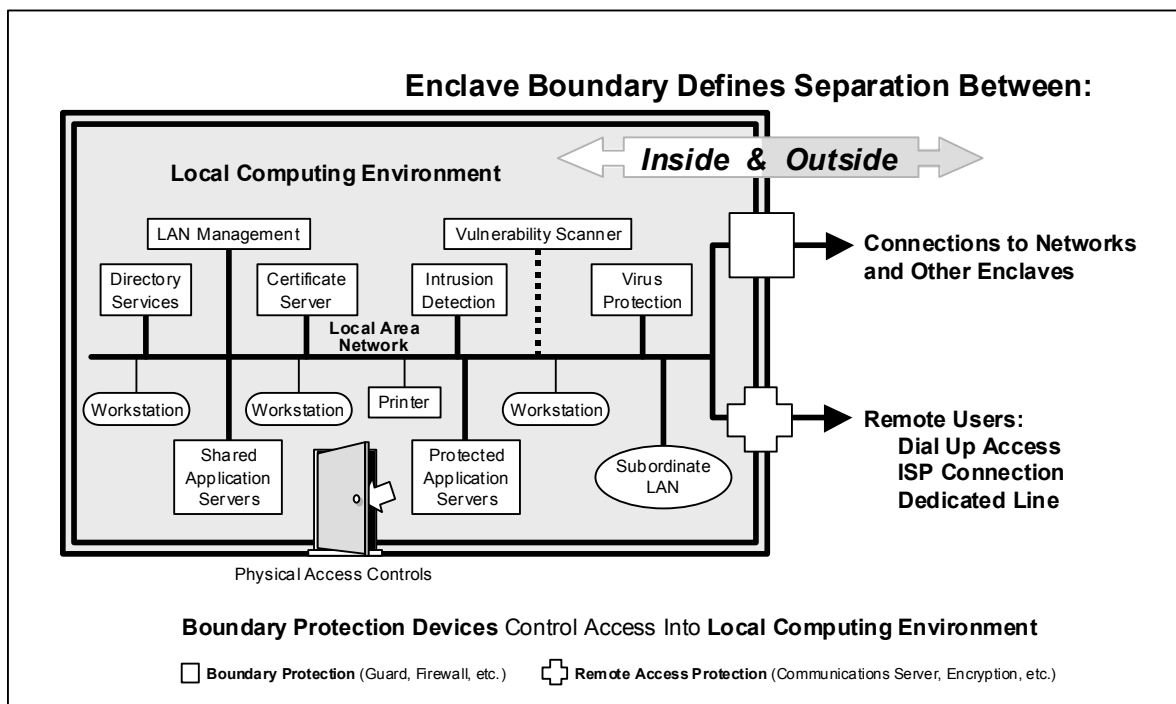


Figure C-3. Defending the Enclave Boundary

(2) Security Management. Enclave perimeters must be established and equipped with professionally managed electronic access portals that enable effective control and monitoring. These portals should use intrusion detection and enable dynamic quality of service (QoS) to rapidly respond to changing

INFOCONs levels. Additional detection mechanisms are required for mission-critical and mission-essential enclaves.

b. Defending the Enclave Objectives

- (1) Ensure that physical and logical enclaves are protected.
- (2) Enable dynamic QoS enforcement due to change in risk posture, local threats, or resulting from changing INFOCONs.
- (3) Ensure that systems and networks within protected enclaves are available and/or usable and are adequately defended against DOS attacks.
- (4) Defend against the unauthorized modification or disclosure of data sent outside or between enclave boundaries with different security policies.
- (5) Provide boundary defenses for those systems within the enclave that cannot defend themselves due to technical or configuration problems.
- (6) Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.
- (7) Provide strong authentication of users sending or receiving information from outside their enclave.
- (8) In order to adequately defend against intrusions, ensure an alarm mechanism is employed to alert the administrator of potential attacks or system crashes.

c. Technology to Defend the Enclave Boundary. This is geared toward ensuring that all outside systems that seek access meet the enclave security criteria. Boundary defenses protect inside data and services from outside dangers. They also protect systems within the enclave that do not have their own self-defense capabilities. Some of the applicable technologies are:

- (1) Identification and authentication tools, such as PINs, passwords, public key infrastructure (PKI) certificates, and biometrics mechanisms.
- (2) Firewalls and routers.
- (3) Malicious code and virus detectors.
- (4) Intrusion detection and response tools (see Appendix N of this enclosure, "Intrusion Detection").

(5) Mail guards, proxy servers, and mail relays.

d. Security Requirements

(1) Boundary Protection Security Requirements

(a) Traffic filtering between internal and external networks will be employed and is typically made on the source address, destination address, transport layer protocol, source port, and destination port. Where required, it may also be filtered on authentication information and stated classification of traffic.

(b) For virus checking, use products from the DOD standard antivirus contract and download and install updated virus detection signatures daily as available.

(c) Only the authorized administrator has the authority to change security policy rules for boundary protection devices.

(d) Users and administrators will be adequately trained, held accountable for their actions, given appropriate privileges, and use system resources for authorized purposes only (See Appendix B of Enclosure A, "Training, Education, and Certification," for training requirements).

(e) Information will not flow between the internal and external networks unless it passes through a firewall and is monitored by an IDS. (Exception: Authenticated, encrypted protocols such as VPNs and secure sockets layer (SSL) pass through the firewall; however this should be evaluated on an individual basis.)

(f) Users will not access firewall configuration software from external networks.

(g) Data packet filtering routers and protected gateways and/or firewalls are required between internal networks and the NIPRNET. Demilitarized zones (DMZs) are required unless no public services or internal access to external users are provided.

(h) Critical systems audit trails should be monitored daily. Audit logs should cover failed log-on attempts, concurrent log-ons, log-on during off-hours, and log-on from users at foreign or unknown locations, file access denials and failed permission changes.

(i) Administrators will successfully authenticate before any transaction on their behalf is allowed.

(j) Only authorized administrators have permission to change security policy on the firewall.

(k) Users on the internal and external side of the firewall are required to authenticate. Users on the external side of the firewall are prohibited from using clear-text services that could lead to potential password compromise (Exception: Use of an anonymous FTP through DMZ).

(l) Only the administrator can access the firewall administration interface remotely. An authorized administrator's ability to remotely access the firewall should be avoided and, if allowed, only on a strictly or conditionally limited basis.

(m) Accounts will lock after a specified number of unsuccessful log-in attempts and an administrator is required to unlock the account.

## (2) Filtering Security Requirements

(a) Sources and executable services will be restricted. A router access control list provides a basic level of access control over network connections based on a site's local security policy. This includes restrictions on incoming and outgoing connections as well as on connections between LAN segments internal to the site and/or enclave. Implement router access control lists based on a policy of "deny by default" with blocks on all services and protocols not required or authorized by the site or workstation.

(b) All networks will employ content security checking mechanisms for all incoming and outgoing files. For virus checking, consider using products from the DOD standard antivirus contract, and download and install updated virus detection signatures as required.

## (3) Layering Security Requirements

(a) E-mail address books will be protected from access by unauthorized personnel. Personnel outside the enclave boundary will be approved by the system administrator before being given specific authority to have access to a network address book.

(b) Establish at least one DMZ within the enclave security architecture either between the perimeter or boundary router and the internal filtering router or firewall. The DMZ will include all systems that are public-



25 March 2003

accessible (e.g., public web servers, mail servers, and external DNS) and be monitored by an IDS.

(c) Proxy services are required to isolate the inside environment from the outside environment while still maintaining an information source for users inside the enclave. Web proxy services will be provided as a minimum.

(4) Connecting Security Requirements

(a) All C/S/A network protection devices must comply with the DOD ports and sockets registry as maintained by DISA (Appendix L to this enclosure, "Ports and Protocols Management Process" (TBP)).

(b) Differentiation between access to networked resources (e.g., router access controls) and user's access to applications must be clearly delineated.

(5) Intrusion Detection Security Requirements. IDS solutions will be in accordance with the NSA protection profiles located on the IATF Forum website ([www.iaf.net](http://www.iaf.net)). See Appendix N of this enclosure, "Intrusion Detection," for discussion on IDSs.

(6) Network Visibility Security Requirements

(a) Provide automated status of LAN configuration and health.

(b) Identify and authenticate all connections.

(c) Provide routine security configuration status checking by using a security configuration application checker (such as DISA or NSA security implementation guides), when appropriate.

(d) Verify all connection configurations at least semiannually or when changes are made.

(7) Remote Access Security Requirements

(a) All remote connections will be identified, authenticated, and logged.

1. DOD PKI keyed, cryptographic-based authentication performed at the enclave boundary will be employed to ensure only authorized users have access to the network.

2. The authentication mechanism should provide mutual authentication of the remote user and the enclave's boundary protection mechanism.

(b) Modem Pools for Dial-up Connections to LANs

1. Modem pools will be located in controlled areas for physical protection and connected to a remote access server to provide electronic authentication of all incoming calls. Connections to modem pools will be logically located in a DMZ.

2. The remote access server will be configured within the security architecture to accept and authenticate calls from the modem pool prior to making connection to the requested information system.

3. All connections will be routed through a filtering router and/or firewall.

4. Physical protection will be provided to prevent unauthorized device changes.

5. Telephone lines for modem pools will be restricted and configured to their mission-required purpose of inward dial only or outward dial only. All modem lines will be restricted to single-line operation and configured without any special features such as call forwarding.

6. Automatic number identification will be used, if available, to enable review of the modem call logs on a periodic basis.

(8) LAN Interconnects Security Requirements

(a) Protect Information. Mechanisms will be employed to ensure information with a higher classification cannot be moved from a system high network to one operating at a lower security level.

(b) Detect and Filter Malicious Code. Mechanisms will be employed on interconnects to identify and remove malicious code prior to passing information between networks.

5. Establish Supporting Infrastructure

a. All military organizations and operations, including IA, require trained, organized structure and processes to provide essential resources and support for maintenance, repair, and other vital services. Many of these services are

25 March 2003

provided across garrison and deployed environments. Supporting infrastructures provide the foundation upon which IA mechanisms are used in the network, enclave, and computing environments for securely managing the system and providing security-enabled services.

b. The infrastructure foundation for protecting DOD information and information systems includes:

(1) Detection, Reporting, and Response. Such infrastructures are essential in discerning whether an intrusion is a local, isolated event or part of a more widespread, sustained, or dangerous attack. The Department of Defense's existing decentralized (distributed) warning and reporting approach helps to ensure that intrusion detection tools and applications at all levels (local, regional, and national and/or global) provide the necessary reports and reporting outputs for the DOD chain of command. Intrusion detection reporting provides specific event and/or activity details to specialized IA and CND facilities (e.g., CERT, NOSC) for analysis and correlation from a range of sources and agencies. Efficient operation of this infrastructure requires standardized reporting formats and procedures, automated support to transfer and analyze relevant data, and effective interface with other response capabilities.

(2) Cryptography. The cryptography function must be resourced and managed to meet requirements without disclosure or theft of key cryptographic information. Equipment and its associated software must be designed and fielded to be reliable, fast, and secure. There must be a cryptographically strong system to produce, distribute, and manage public and private keys for classified systems (electronic key management system for high assurance crypto and SIPRNET PKI for need-to-know enforcement and authentication) and unclassified systems (DOD PKI).

6. Defense-in-Depth Examples. To illustrate the defense-in-depth strategy, the following paragraph provides examples of using layers of security services implemented in the four areas to create a stronger defense than a single component could provide. Note that these are examples only. An acceptable security solution for any particular environment depends on the existing threats and the acceptable risks. When implementing solutions, approved NSA protection profiles will be used where available and when appropriate. For solutions involving classified information, only NSA-approved, high-robustness solutions may be used. In all cases, only national information assurance partnership (NIAP)-validated products (or those migrating to NIAP standards), configured in accordance with security policy and well maintained, will be considered as part of the solution as determined by IATF guidance and information system security engineering of the requirements. The suggestions

25 March 2003

below are by no means comprehensive. They represent only a short list of some of the more common means of accomplishing defense-in-depth.

a. Defending the Network and Infrastructure. This area covers the network backbones and the infrastructures that allow those backbones to serve individuals and organizations. Components found in this area include switches, routers, DNS servers, and link encryptors. Confidentiality and availability services are often provided by IA components in this area. When defense is built in-depth, the defensive foundation layer often resides here. The objectives and recommended potential countermeasures in this area are:

(1) Ensure that all data exchanged over WANs is physically or cryptographically protected from disclosure to anyone not authorized network access.

(a) This requires application of the confidentiality service, which, in general, is accomplished using NSA high-robustness cryptography for classified data and approved basic or medium robustness commercial solutions for unclassified sensitive data as indicated in Appendix H to Enclosure C, "Protection Mechanisms – Levels of Concern and Robustness."

(b) Consider the case where multiple SBU LANs are connected via the NIPRNET. These connections between communities of interest can be protected with a VPN, such as Internet Protocol Security (IPSec) that meets the basic robustness level.

(c) Well-configured routers on the backbone, using secured routing protocols, can make it difficult to reroute and intercept packets. Imagine the task for an adversary if data encryption using IPSec were required of all communications between any two networks that are in the .gov or .mil domains. If an adversary only has access to the transmission medium they would have so much encrypted traffic to sort through that it would be difficult to identify just one particular type of message to target.

(2) Ensure that WANs supporting mission-critical and mission-support data provide appropriate protection against DOS attacks.

(a) Medium-robustness mechanisms must be implemented to ensure positive control of all mission-critical network elements. Inbound remote management of all critical network elements requires authentication, confidentiality, and integrity protection for all network management transactions and enclave boundary protection for centers that manage the control of the WANs. Basic robustness may be sufficient for encrypted WANs.

(b) DOS attacks can be targeted at an end system (perimeter), or at part of the infrastructure, like the routers. A defense-in-depth solution against a router DOS attack is to configure independent redundant or backup connections to the network infrastructure.

(c) Another mechanism is to establish a security perimeter and require edge devices to disallow external network management traffic.

(3) Protect against the delay, misdelivery, or nondelivery of otherwise adequately protected information.

(a) QoS protocols can be employed in the network infrastructure and at the enclave boundary to reserve bandwidth. Properly configured QoS mechanisms can provide another layer of defense for the availability service.

(b) DNS is a critical service that allows enclaves to locate each other across the network infrastructure. One could defend DNS servers by placing them in multiple locations, connected independently.

(4) Protect from traffic-flow analysis, both user traffic and network infrastructure control information.

(5) Ensure protection mechanisms do not interfere with otherwise seamless operation with other authorized backbone and enclave networks.

b. Defending the Enclave Boundary. This area covers the points where data passes between enclaves and the network infrastructure. The enclave boundary is important because it supports application enclave-specific policies and security services. Authentication, access control, confidentiality, and availability services are all part of the defense at the enclave boundary, to include firewalls, routers, remote access servers, guards, and IDSs. The objectives of defending the enclave boundary are to:

(1) Ensure physical and logical enclaves are adequately protected.

(a) A proxy firewall can be placed at the enclave boundary, reinforcing the access to the individual computers within the boundary, limiting outsider access, and providing a separate audit trail.

(b) A router outside the firewall can filter to allow expected types of packets and deny all others. This limits the options an opponent has to defeat the firewall, using the router as a first component to layer with the original firewall.

(c) Firewalls, meeting the basic robustness level and configured in accordance with DOD firewall policy, provide adequate protection for single-level, same-classification-level connections (e.g., SECRET US ONLY to SECRET US ONLY, UNCLASSIFIED to UNCLASSIFIED). MAC I systems should select solutions achieving the medium robustness level.

(d) Connectivity across security levels (e.g., TOP SECRET to SECRET, SECRET to UNCLASSIFIED, US ONLY to foreign-nation systems) will be implemented only due to operational necessity and in accordance with an official process, such as the SABI and TSABI. This connectivity, which commonly has a guard, must achieve the high-robustness level to protect the higher-classified network's information. (All boundaries between enclaves and WAN will contain an intrusion detection and/or attack sensing and warning capability.)

(2) Ensure dynamic control of services in response to changing threats.

(3) Ensure that systems and networks within protected enclaves are available to both internal and external users and are adequately defended against DOS attacks.

(4) Ensure that data exchanged between enclaves or via remote access is protected from improper disclosure.

(a) Remote access connections to unclassified networks require authentication with techniques, such as nonreusable passwords, PKI and public key encryption, or other recommended encryption technologies.

(b) When exchanging classified data across unprotected networks (SECRET data across the public phone system as in the remote access example), then there is a need for enclave boundary protection to protect the secret enclave.

(c) When lower security levels use a higher security level backbone (e.g., SECRET through TOP SECRET, UNCLASSIFIED through SECRET), data separation may be accomplished using medium-robustness algorithm. In addition, there is a need for enclave boundary protection of the higher-level backbone.

(5) Provide boundary defenses for those systems within the enclave that cannot defend themselves due to technical or configuration problems.

(6) Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.

(7) Protect against external systems or forces undermining protected enclave systems and data.

(a) Filtering can be done at the gateway between networks of the same classification level to permit only valid connections to enter into the LAN, filtering either by IP address, or by stronger identification mechanism, such as a VPN. Knowing the connection identification information provides an additional way to limit access beyond that of user identification.

(b) Mechanisms at the enclave boundary should be established and maintained to scan for malicious software entering or leaving the enclave (i.e., virus scanners).

(8) Provide strong authentication, and thereby authenticated access control, of users sending or receiving information from outside their enclave. Use medium-robustness solutions to authenticate the transfer of data between enclaves.

c. Defending the Computing Environment. This area includes user computers, servers, printers, databases, etc., that provide local support to mission functions. All security services are provided in this area. The objectives and example countermeasures in meeting this area are:

(1) Ensure that client servers and applications are adequately defended against DOS, unauthorized disclosure, and modification of data. One defense of a client against a DOS attack is by filtering at the boundaries to prevent the adversary from being able to send enough packets to bring down a client. For example: an intelligent filtering capability would allow a boundary device to discard synchronous idle character (SYN) flood packets by looking at the transaction history and verifying whether the incoming SYN is expected or not. Authentication can help ensure only legitimate users access a resource, letting the server do a less resource-consuming authentication before performing the more consuming service.

(2) Ensure the confidentiality and integrity of data processed by the client, server, or application whether internal or external to the enclave by using signatures and basic or medium robustness encryption.

(a) Many protocols, such as transmission control protocol (TCP) and/or Internet protocol (IP), include a check sum to prevent the inadvertent changing of data in transit. The check sum within TCP/IP protocol is primitive in terms of security robustness; however, when used in conjunction with other stronger-integrity mechanisms, it can contribute to defense-in-depth.

(b) One method for detecting modification of data is a check sum or hash on the stored data that can be computed and saved for later verification of the data.

(c) Digital signatures add cryptographic enhancements to hashes and/or digests further enhancing data integrity capabilities. All individual E-mail and E-commerce transactions (unclassified but sensitive) will be secured with a digital signature implementation at the basic-robustness level for mission support and administrative information and the medium-robustness level for mission-critical information. Digital signatures within a system high, classified environment require, at a minimum, basic or medium robustness.

(d) Confidentiality of information in transit can be achieved through encryption or a protected distribution system. Classified information requires high-robustness solutions, while unclassified-but-sensitive information requires basic-robustness solutions.

(3) Defend against the unauthorized use of a client, server, or application.

(a) User authentication mechanisms for workstations (e.g., log-in) must meet a basic level of robustness. The most common form of user authentication is the password. Strong passwords are recommended. Defense-in-depth uses factor authentication mechanisms that comprise two of the following factors:

1. Something you know (e.g., password).
2. Something you have (e.g., token).
3. Something you are (e.g., biometrics).
4. Something you can do (e.g., write your signature).

An example would be possession of a hardware token and knowledge of a PIN or some other type of password.

(b) Biometrics could be combined with the above example to form an additional layer of user authentication. For example, a user might be required to pass biometrics authentication at the enclave boundary, then supply a password for access to a database within their computing environment.



(c) Basic-robustness authenticated-access solutions are required for user access to servers (e.g., web servers, database servers, or file servers) or other components storing special compartmented, special access, or other mission-critical information, if the underlying network infrastructure is already encrypted and/or physically isolated. User access to servers (e.g., web servers, database servers, or file servers) or other components storing mission support or administrative information will use basic-robustness-authenticated access. Any other user access will require a medium-robustness authenticated access solution.

(d) The sender of a document can provide nonrepudiation and verify integrity by digitally signing the document.

(4) Ensure that clients and servers follow secure configuration guidelines and have all appropriate patches applied.

(a) Proper SA training and certified system administration policies can increase the security of a network.

(b) A good client/server configuration is itself a layer of defense-in-depth and can provide access control in the following ways:

1. Users are created with certain privileges and placed into groups that also have privileges. Users are given privileges based upon access requirements to the information, and this is referred to as the least-privilege principle. Where possible, SA and security administrator roles should be separated.

2. Files are placed into directories, both of which have access lists that state which users and groups can access files.

3. Applications are regularly patched to eliminate any discovered vulnerability that could be used to elevate the access level of the user.

4. Unused services are turned off to help prevent unauthorized access to the client and/or server.

(5) Maintain CM visibility of all clients and servers to track patches and system configuration changes.

(6) Ensure that a variety of applications can be readily integrated with no reduction in security. It may not be possible to combine some security

25 March 2003

mechanisms to achieve defense-in-depth. For example, providing confidentiality by encrypting every message on a LAN between two clients, but also running an IDS on the local LAN, will not achieve defense-in-depth because the encryption mechanism defeats the intrusion detection. Intrusion detection requires access to the plain text messages to search for known attacks, and if all the traffic were encrypted, it would not be able to spot vulnerabilities for which it is searching. In this case, defense-in-depth demands that IDS capabilities be implemented on the host/server or in the application.

(7) Ensure adequate internal and external defenses and accountability measures against subversive acts of trusted people and systems.

(a) Physical security, background investigations of trusted employees, and security training add to the security of the network. This is an example of nontechnical defense.

(b) SAs access to network management centers and network management control commands used to manage components (e.g., routers and switches) and access lists to clients and servers require basic-robustness authenticated access if the underlying network infrastructure is already encrypted and/or physically isolated. Any other system administration activities will require medium-robustness-authenticated access.

d. Establishing Supporting Infrastructure. This area covers mechanisms and techniques that enable or bind together security components in other areas. Some of the components found in this area include PKI servers (e.g., certificate authorities and directory servers), attack sensing and warning systems, and key management systems. The objectives and some examples in meeting this requirement are:

(1) Provide a cryptographic infrastructure that supports key, privilege certificate management, and enables positive identification of individuals using network services.

(a) Provide a good certificate-issuing infrastructure for legitimate users, and protect certificate private keys that have been issued.

(b) Authentication and access control play an important role in the use and management of PKI. Basic to high-robustness solutions must be applied appropriate to the types of symmetric and asymmetric key being created, distributed, and managed by the infrastructure.

(c) Digital signatures will be applied to information stored in the directory to provide for integrity.

(d) Trusted third party authentication can be used to provide some nonrepudiation capability.

(2) Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that enables rapid detection and response to intrusions and other anomalous events, and enables operational situation awareness.

(a) Once firewall protocols are defined, an intrusion detection tool can scan permitted protocols for malformed packets.

(b) Network and host-based sensors and vulnerability scanners, malicious-code detectors, war dialers, and file integrity checkers should be deployed to provide attack protection and facilitate policy enforcement.

e. Defense-in-Depth Solution Example. A real-life defense-in-depth solution is an implementation of a remote access security program (RASP) for SBU data. RASP enables traveling or telecommuting users to securely access their LANs, enclaves, or enterprise-computing environments via telephone networks. The communication network is untrusted and may be shared with hostile users. The remote user's computing assets are physically vulnerable, especially when outside the United States, and must be protected. This equipment should be unclassified when not in use. In addition, the user should know when security features are enabled, and more importantly, when they are not. The RASP for SBU data combines technical and nontechnical mechanisms to implement its solution. Figure C-4 depicts a typical RASP configuration, which contains the components needed to protect SBU data. Threats and technical RASP solutions include:

(1) **Threat:** Eavesdropping on unsecured public telephone lines.  
**Solution:** Encrypt all transmitted plain-text data between the remote laptop and the RASP secure access server, thus preventing plain-text data from being monitored or intercepted by others. Encryption is provided by the USG-approved FORTEZZA<sup>®</sup> modems in the remote laptop and RASP secure access server. The SKIPJACK algorithm and key exchange algorithm are implemented in the FORTEZZA<sup>®</sup> modems and approved basic-robustness solutions. In addition to the FORTEZZA<sup>®</sup> encryption, access to the web server from the remote laptop provides an additional layer of encryption using SSL protocol (if enabled).

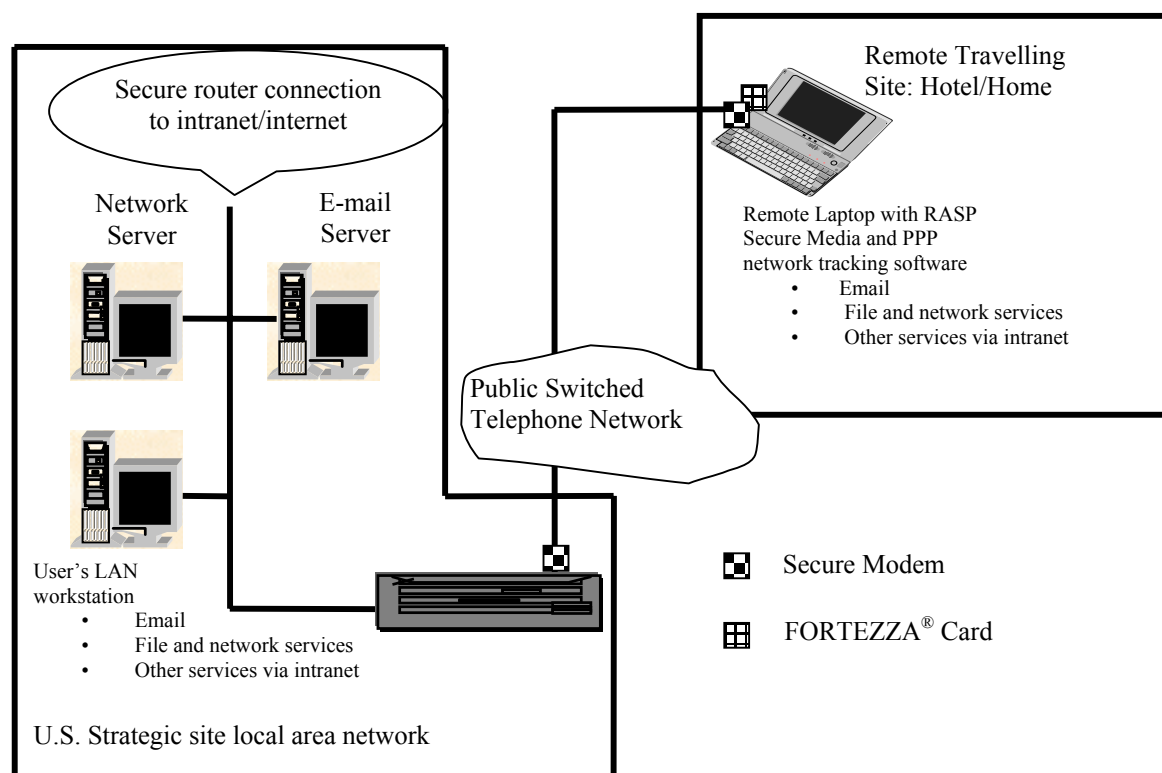


Figure C-4. Typical RASP Configuration

(2) **Threat:** Loss or theft of portable computers. **Solution:** Encrypt sensitive information on the remote laptop's hard drive, rendering it inaccessible by thieves. RASP secure media application in conjunction with the FORTEZZA® card is used to encrypt all data stored on the remote laptop's hard drive. Using E-mail encryption for sensitive messages provides another layer of defense when the messages are stored on the remote laptop in encrypted format. In addition, tamper seals can be used to indicate when potential loss of data occurs due to a laptop being temporarily out of the user's control (e.g., customs and airport inspections).

(3) **Threat:** Unauthorized access to an SBU LAN. **Solution:** Prevent unauthorized persons from accessing an SBU LAN with effective, two-factor authentication that requires a user's PIN to access the properly configured FORTEZZA® card. Once the user gains access to the LAN, the user needs to self-authenticate to the computing resources on the LAN (e.g., account log-ins). This provides an additional level of access control to the resources.

(4) The above RASP solutions have various configurations and when configured correctly and used in conjunction with the security policy and operational doctrine, RASP can be used for transmission of SBU data. Upon

25 March 2003

local DAA approval of the solution, the DSAWG may approve SIPRNET access when following the FORTEZZA<sup>®</sup> for classified policy.

7. Guidance. STIGs and other technical guidance can be found at <https://iase.disa.mil/documentlib.html>. The STIG is a compendium of security regulations and best practices from many sources that apply to an operating system or a part of the GIG infrastructure. This web site provides security technical guidance on a number of topics (Windows XP, Windows 2000, Windows NT, Cisco Router, UNIX, databases, Unisys, Tandem, Novell NetWare, networks, Web, E-mail and additional topics).

(INTENTIONALLY BLANK)

## APPENDIX A TO ENCLOSURE C

## AUTHENTICATION

1. Authentication. This appendix outlines minimum implementation requirements for authentication of individual users on DOD information systems.
2. System Access. The user is required to authenticate themselves before being allowed access to the system. Password-protected screen savers should be used if available on system.
3. Password Ownership
  - a. A personal password, not a system level password, will be individually owned, rather than owned in common by a group of individuals to provide individual accountability within a computer system.
  - b. Individual ownership of personal passwords is required to:
    - (1) Establish individual accountability to determine who accessed what resources, when, and for what purposes.
    - (2) Establish illicit use of a password or loss of a password.
    - (3) Be used for an audit trail of the activities of a user.
    - (4) Avoid the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges.
  - c. When possible, use a password enforcement program to verify a password complies with the password policy.
  - d. Passwords are linked to personal accounts with varying levels of access. Personnel granted authorized access to DOD computer systems or networks will not share passwords or account access. This includes supervised or unsupervised usage by persons not assigned to the account.
4. Password Format. Passwords will be at least eight characters long and consist of a mix of uppercase letters, lowercase letters, numbers, and special characters, using three of four character sets. Note: Eight characters are the DOD minimum requirement. If technically feasible, 12 to 16 characters using a mix of all four-character sets is recommended. (e.g., 14 characters using a

mix of all four-character sets in the first 7 characters and the last 7 characters).

5. User Validation. User is required each time a user logs onto the system, either initially or after a screen lock program is interrupted.

6. Password Protection

a. Passwords must not be displayed at any terminal or printer.

b. The user will employ appropriate actions to prevent disclosure while logging-on to system.

(1) Practice entry of the password so that it can be quickly entered.

(2) Shield the keyboard to prevent the observer from seeing the keys being pressed during password entry.

(3) Request a guest not watch the password entry process.

(4) Log-on prior to demonstrating use of the system.

7. User Maintenance. Passwords must be changed or invalidated at least every 90 days or less for classified systems (e.g., SIPRNET) and for controlled-but-unclassified systems (e.g., NIPRNET). Organizations may consider shorter periods for user or SA passwords on sensitive systems requiring greater security.

8. Storage

a. Passwords will be stored in the authentication system that minimizes their exposure to disclosure or unauthorized replacement.

b. Encryption of electronic-stored passwords and password files is required.

c. Passwords will never be part of the boot process or be executed via function keys.

d. Password Vaults

(1) A password vault is a utility program that stores multiple passwords under a master password. This eliminates the problem of users forgetting multiple passwords or having to write them down.



(2) The use of a password vault will only be considered if:

(a) Passwords are stored by a minimum of 128-bit encryption.

(b) The vendor provides a Vendor Integrity Statement.

(c) The IAO or IAM approves the software and use of this product is reflected in the system accreditation.

e. Default directory names will be changed to prevent easy targeting by automated password cracking programs.

#### 9. Authentication Failures

a. Users will be allowed no more than three attempts to log onto system. After the maximum number of attempts is exceeded, the account must be locked.

b. If technically feasible, the system will also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. The system may also allow passwords to reset after a given amount of time (e.g., 15 minutes). This prevents an automated, high-speed DOS via account lockout attack on the password system.

c. Ideally, the log-on prompt will immediately go to the password prompt. If an unsuccessful logon has taken place, there will be no indication as to whether the log-on ID or password caused the failure.

d. A security record will be maintained of the passwords entered incorrectly, but the incorrect password should not be kept in the record. A security alarm should be generated if:

(1) The maximum number of allowed account password retries is exceeded.

(2) The maximum number of allowed failed log-ons from one terminal is exceeded.

(3) The maximum number of allowed failed log-ons for a period is exceeded.

e. The above security parameters must be set according to the sensitivity of the data being protected, the profile of the typical system user, and the policy of the organization.

f. User accounts will be disabled, and users should be denied service if these parameters are exceeded. The SA should be the only one who can reset the account and restore the service of the user following these events.

g. The system should inform the user, following a successful log-on procedure, of the date and time of the last successful access by the user and any unsuccessful intervening access attempts. The notification should not scroll by but remain on the screen until another keystroke is entered giving the user a chance to view the statement. This will aid in uncovering any unauthorized accesses or attempted accesses that may have occurred between authorized user accesses.

10. User Password History. A history of individual password usage will be maintained for 1 year to preclude the use of old passwords. Users or SAs will not be able to reuse any of the last ten previous passwords. If a password history file is not available, the SA should audit password activity to ensure that no individuals use any of their last eight passwords.

#### 11. Memorizing Passwords

a. Users will memorize their passwords; however, if it is necessary to maintain a password list it must be kept secured.

b. Users are encouraged not to keep a copy of their written password, but it is often necessary to have it available. The password should be protected as follows to prevent loss and to detect a compromise.

(1) Do not store the password where it is easily accessible to computer.

(2) Do not keep the password and user ID together.

(3) Store the password in a locked drawer, cabinet, or container.

(4) Seal the password in an envelope and sign across the seal to detect tampering.

#### 12. Disclosure of Passwords

a. Users will not disclose their passwords to anyone.

b. Disclosing a personal classified system password to anyone without a valid clearance and need to know constitutes a security violation.

c. Disclosing an account password or permitting unauthorized use of a DOD computer system or network constitutes a security violation. Authorization for computer network use may be obtained only from those personnel granted such authority by the DAA.

13. Compromised Passwords. Users must immediately notify the SA or IAO if it is believed that a password has been compromised.

14. Unclassified System Access

a. SAs will not share unclassified system access passwords.

b. Unclassified system access passwords maintained on paper will be sealed in a Standard Form 700 or plain envelope and protected.

15. Classified System Access

a. SAs will not make classified system passwords available to anyone, including other SAs.

b. Classified system access passwords maintained on paper will be sealed in a Standard Form 700 and stored in a secure container with access to those with need to know.

16. Factory-Issued Identifiers or Passwords. All factory-set, default, or standard-user IDs and passwords will be removed or changed prior to the system going operational. Afterwards, systems will be rechecked periodically to confirm upgrades or patches have not reinstalled factory password defaults or other types of backdoors.

17. Conditions Requiring Password Changes

a. Passwords will be changed when compromised, possibly compromised, forgotten, or if suspicious activity on an account appears in an audit log.

b. Group passwords are discouraged; however, in some watch-standing or administrative situations, DAAs may approve use conditionally. If a group password is authorized and created, the password must be changed when compromised or a member of the group leaves.

18. Disabling Accounts

- a. User IDs will be removed or reassigned within 2 days of notification that a user no longer requires access to the system.
- b. Users and supervisors are responsible for notifying SAs or IAOs when access is no longer required.
- c. SAs will suspend user IDs and passwords that have not been used in a 30-day period.
- d. User accounts will be disabled immediately upon identification of unauthorized activity by user.

19. Classification and Control of Passwords

- a. All passwords of unclassified systems will be treated as sensitive and secured appropriately.
- b. Passwords of classified systems will be classified at the accredited classification level of the system and secured appropriately.

## APPENDIX B TO ENCLOSURE C

## FOREIGN ACCESS TO INFORMATION AND INFORMATION SYSTEMS

1. Procedures

a. Connection (access) by foreign nationals (i.e., a person who is not a citizen of the United States) to a DOD-owned or DOD-managed information and information system, including information systems or networks operated by contractors under a DOD contract, will be controlled. Controls must prevent unauthorized (intentional or unintentional) access, disclosure, destruction, or modification to the information or the information system.

b. Disclosure of classified information and controlled unclassified information to foreign governments and international organizations is limited and will be in accordance with National Disclosure Policy (NDP-1) (reference y), DODD 5230.11 (reference z), DODD 5230.20 (reference aa), DODD 5230.25 (reference bb), DODI 5230.17 (reference cc), DOD 5200.1-R (reference i), DOD 5200.2-R (reference a), CJCSI 5221.01 (reference dd), C/S/A guidance, and guidance in this manual.

c. Connections to foreign systems will be in accordance with CJCSI 6740.01 (reference ee), CJCSI 6211.02 (reference c), SABI, TSABI and the GIAP (<http://giap.disa.smil.mil>). The SCAO ([scao@ncr.disa.mil](mailto:scao@ncr.disa.mil) and [scao@ncr.disa.smil.mil](mailto:scao@ncr.disa.smil.mil)) serves as the single POC for SIPRNET connections.

2. Foreign National Access to Information

a. Criteria. Foreign national access to classified information (including classified information received from DOD classified systems) to foreign governments or organizations is limited and will be in accordance with NDP-1 (reference y), DODD 5230.11 (reference z), DODD 5230.20 (reference aa), and CJCSI 5221.01 (reference dd). Enclosure 3 to DODD 5230.11 (reference z) establishes the following criteria for the disclosure of classified information.

(1) Disclosure is consistent with US foreign policy and national security objectives concerning the proposed recipient foreign government.

(2) Disclosure is consistent with US military and security objectives.

(3) The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States.

(4) Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed.

(5) Disclosure is limited to information necessary to the purpose for which disclosure is made. For example, if the purpose of the disclosure were the sale of military equipment, information on operation, maintenance, and training would be released. Research and development data or production know-how must be withheld.

b. Disclosure of Unclassified Information

(1) There are other types of unclassified information that require application of controls and protective measures for a variety of reasons. This information is known as “controlled unclassified information.” The types of information in this category include FOUO information, SBU (formerly “Limited Official Use”) information, “Drug Enforcement Agency Sensitive Information,” “DOD Unclassified Controlled Nuclear Information,” “Sensitive Information” (as defined in the Computer Security Act of 1987), and information contained in technical documents. Appendix C of DOD 5200.1-R (reference i) provides specific guidance on proper handling “controlled unclassified information.”

(2) C/S/As must ensure that a foreign national (Non US citizen) only accesses “controlled unclassified information” authorized for release to the foreign national’s government. Access by foreign nationals to controlled unclassified information will be in accordance with the International Traffic in Arms Regulations (ITAR) (reference ff), the Export Administration Regulations (EAR) (reference gg), DODD 5230.25 (reference bb), and DODD 5400.7 (reference hh).

(a) This includes non-US information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country.

(b) Controlled unclassified information also includes US information that is determined to be exempt from public disclosure in accordance with DODD 5230.25 (reference bb) and DODD 5400.7 (reference hh) or that is subject to export controls in accordance with the ITAR (reference ff) or the EAR (reference gg).

3. Assignment of Foreign Nationals to DOD Organizations

a. Examples of foreign nationals (DODD 5230.20 (reference aa)) assigned include:

(1) Foreign Liaison Officer (FLO). Foreign government military member or civilian employee who is authorized and certified by a DOD component to act as an official representative of that government in its dealings with DOD

25 March 2003

components in connection with programs, projects, or agreements of mutual interest. The three types of FLOs include security cooperation, operational, and national representative(s).

(2) Foreign Exchange Personnel. Military or civilian officials of a foreign defense establishment (a DOD equivalent) who are assigned to a DOD component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DOD component.

(3) Cooperative Program Personnel. Foreign government personnel, assigned to a multinational program office that is hosted by a DOD Component pursuant to the terms of a Cooperative Program International Agreement, who report to and take direction from a DOD-appointed PM (or PM equivalent for the purpose of carrying out the multinational project or program).

(4) Other Foreign Nationals. Foreign nationals that (pursuant to agreement or contract) the Department of Defense has determined require access to information systems (e.g., students assigned to military academies or other DOD schools).

b. The authorization for access will be defined in the Delegation of Disclosure Authority Letter related to assigned foreign nationals.

c. This paragraph does not include foreign nationals that are DOD employees, Service members, or DOD contractors (see paragraph 7 and 8 below).

#### 4. Interconnections to Agencies of Foreign Governments

a. Requests and approval for a foreign connection to DOD information systems will follow the GIAP (<http://giap.disa.smil.mil>). The SCAO ([scao@ncr.disa.mil](mailto:scao@ncr.disa.mil) and [scao@ncr.disa.smil.mil](mailto:scao@ncr.disa.smil.mil)) serves as the single POC for SIPRNET connections. The interconnections will be IAW SABI, CJCSI 6740.01 (reference ee), and CJCSI 6211.02 (reference c). Variations shall be approved by the responsible combatant commander and DISN DAAs and incorporated in the system security documentation.

b. The organization submitting requests for interconnections will provide:

(1) Mission requirement that interconnection supports; and whether the interconnection is in direct support of a coalition partner. Include the primary user(s) (sender and receiver) of the data transferred via the interconnection.

25 March 2003

(2) Mission impact if the interconnection is not authorized (speed or delay in mission accomplishment, staffing effects, hardware and software costs, etc.).

(3) Security domain(s) being interconnected (e.g., SIPRNET to coalition SECRET).

(4) Technology used for the interconnection and the number of devices.

(5) Accreditation status of the interconnected domains (e.g., fully accredited or IATO and date). Note: IATOs have a time limit when issued.

(6) Residual risks identified by the accreditation.

(7) DAA of each local subscriber environment.

(8) Date of the last joint vulnerability assessment process (JVAP) or other electronic evaluation of each local subscriber environment.

(9) Data type(s) passed over the interconnection and data owner(s), including, if applicable, whether attachments are allowed across the interconnection.

(10) Command communications service designators and IP addresses of each side of the interconnection including a JVAP table if available.

(11) An estimate of the volume of information passed across the interconnection.

(12) If applicable, identify the DOD or IC program office that provided the interconnection technology.

c. The initial request will be sent to the SCAO for processing.

(1) The Communications and Computer Networks Division J-6T, Joint Staff will validate foreign connection request and process them for ASD(C3I) approval.

(2) The proposed connection security component will be reviewed by the DSAWG in accordance with CJCSI 6211.02 (reference c). The DSAWG will provide accreditation recommendations (approval or disapproval) to the DISN DAAs.

d. The four DISN DAAs (Director, Joint Staff, Director, DISA, Director, DIA and DIRNSA) will make final interconnection decision.



(1) An approval will include a memorandum of agreement covering such areas as maintenance of security posture, acknowledgement of periodic monitoring, notification of relevant security changes, and periodic reaccreditation.

(2) Disapproval to connect will include specific recommendations and guidance on obtaining approval.

e. System accreditation authorities will ensure strict compliance with GIAP and the SABI and TSABI processes.

f. Approved security devices will be employed on each foreign connection. These security devices must be in US-controlled spaces.

#### 5. Foreign National Individual Access to Unclassified DOD Information Systems

a. Access Requirements. Before authorizing foreign national (Non US citizen) access to specific unclassified information systems, DOD components will:

(1) Ensure DAAs concur in the access and, if the information system contains sensitive information, that the DOD component (C/S/A) head concurs (DODI 8500.2 (reference w)).

(2) Ensure foreign disclosure officer (FDO) reviews information required to support foreign national's duties and that information has been authorized for release to that foreign national's government.

(3) Ensure system certification and accreditation documentation is updated to reflect foreign national access.

(4) Ensure security measures employed adhere to DOD, C/S/A, and local information assurance and system security policy and procedures.

(5) Ensure accountability is maintained through audit trails of all actions taken by foreign national within information system.

(6) Ensure foreign users follow DOD and local security policies and procedures and the IAO is given authority to enforce policies and procedures. Prior to accessing the system, a foreign user will sign a user agreement that includes:

25 March 2003

(a) Acknowledging information and information system security policies, procedures, and responsibilities.

(b) Consequences of not adhering to security procedures and responsibilities.

(7) Ensure that the foreign national is identified when dealing with others through written and electronic communications, such as E-mail.

(a) For E-mail accounts, the user name will include individual's nationality. If a commander or agency head determine operational and/or security concerns preclude use of specific nationality for an individual then generic designation of "FN" (foreign national) will be used and documented.

(b) Format is as follows:

1. Use the federal information processing standard (FIPS) 10-4 (reference ii) codes for country designations in the simple message transfer protocol (SMTP) address.

2. Use full country name in the E-mail alias.

3. The alias format is name, country, and duty description.

4. The SMTP format is name.FIPS countrycode@C/S/A.mil.

(c) Format examples:

1. Alias – John Doe, Australia, LNO, Combatant Command  
SMTP – john.doe.as@combatant command.mil

2. Alias – John Smith, United Kingdom, FLO, Service  
SMTP – john.smith.uk@service.mil

(d) Auto E-mail signature blocks shall be used and will include foreign individual's name, nationality, duty description, and organization assigned. Format example: Doe, John WG CDR, United Kingdom–FLO, combatant command, J6.

(8) Ensure the foreign national abides by the C/S/A Certification Practice Statement (CPS) to obtain and use the PKI certificate(s) necessary for access to unclassified information systems.

b. NIPRNET access requirements (access to DOD.mil enclave from another DOD.mil enclave or .mil E-mail address) for foreign personnel, outlined in paragraph 3 above, are delegated to C/S/As for approval. C/S/As will ensure access requirements (networks and **information**) in subparagraphs 2b and 5a (above) are implemented. Accountability is crucial.

## 6. Foreign National Access to Classified Information Systems

### a. Control of US-Only Classified Networks and Terminals

(1) Foreign nationals will not be granted access to US-Only classified networks and terminals (e.g., US Only Enclaves on SIPRNET).

(2) Terminals and network equipment will remain under strict US control at all times.

(3) When classified terminals are located in workspaces physically accessible by foreign nationals (such as combined operations centers), classified terminals must be grouped together in a US-controlled terminal space.

(a) If the grouping of US-only classified terminals at a site is not operationally possible, the following steps will be taken by the responsible C/S/A element:

1. The US command or agency will authorize an exception at the site, in writing, stating operational reasons for exception, and maintain the record of exception.

2. The site will develop, publish, and maintain written procedures on security measures to safeguard US-only classified terminals.

3. Ensure that US personnel are briefed and enforce security measures.

(b) As an additional precaution, screen savers with password protection must be used on all classified terminals in combined workspaces.

(4) If foreign national is permitted access to the US-controlled terminal space, the individual must be announced, screens must be covered or blanked, the visitor must wear a badge clearly identifying them as a foreign national, and the individual must be escorted at all times.

(5) If the foreign national is permitted to view the screen, US personnel must ensure:

25 March 2003

(a) Information is releasable in accordance with C/S/A guidance and will be consistent with NDP-1 (reference y), DODD 5230.11 (reference z), DODD 5230.20 (reference aa), DOD 5200.1-R (reference i), and CJCSI 5221.01A (reference dd).

(b) Foreign national has security clearances granted by their government at a level equal to that of the classified information involved and an official need to know.

b. SECRET E-mail Capability. Before authorizing foreign national personnel SECRET E-mail capability DOD components will:

(1) Implement information system interconnection requirements outlined in paragraph 4 and individual access requirements in subparagraph 5a.

(2) The classified information system used by the foreign national will be connected through an approved interconnection to ensure that access to classified and controlled unclassified information is strictly limited (i.e., dedicated workstations) within a coalition wide area network (CWAN). The connection will be via approved guard technology to support E-mail with attachments and other DISN DAA approved technology. All other access capabilities to or through the SIPRNET, such as web browser, will be rendered inaccessible.

(3) The CWAN or dedicated workstation extension will be accomplished via approved Type I encryption across the SIPRNET and SABI approved security architecture to support E-mail capability.

(4) Requests and approval for SECRET CWAN connection or dedicated workstation will use the GIAP through the SCAO (scao@ncr.disa.mil and scao@ncr.disa.smil.mil), in accordance with CJCSI 6740.01 (reference ee), and CJCSI 6211.02 (reference c).

(5) Approval for allowing E-mail attachments by specific type will be through the DSAWG with final approval by the DISN DAAs.

c. Coalition WANs

(1) Release of Information

25 March 2003

(a) Information E-mailed to coalition network members will be releasable in accordance with NDP-1 (reference y), DODD 5230.11 (reference z), CJCSI 5221.01A (reference dd), and bilateral agreements.

(b) Information accessible to all coalition network members (e.g., web page or database) will be identified as coalition-releasable and in accordance with NDP-1 (reference y), DODD 5230.11 (reference z), DODD 5230.20 (reference aa), CJCSI 5221.01A (reference dd), and multinational agreement(s) (e.g., NATO).

(c) FDO will review and concur that information is required to support foreign national's duties and has been authorized for release to that foreign national's government.

(2) The GIAP through the SCAO (scao@ncr.disa.mil and scao@ncr.disa.smil.mil) will be used for interconnection between a coalition network (enclave) and US-only classified information systems or enclaves (networks) at SECRET-level.

(3) Common basic security requirements and procedures will be developed for coalition networks based on security risk assessments.

(4) Users will be informed of information and information security requirements of the coalition network. Individual user agreements may be appropriate.

#### 7. DOD Foreign National Employees and Foreign National Service Members as Authorized Users

a. Access to DOD-owned or DOD-managed information systems is authorized for controlled unclassified information systems on a need-to-know basis for official duties by DOD foreign national employees (Non US citizens) and foreign nationals (Non US citizens) serving with a US military service (active duty and reserve).

b. DOD foreign national employees with authorized user access to DOD information and information systems will comply with requirements of DODI 8500.2 (reference w) and DOD 5200.2-R (reference a).

c. Foreign national employees will meet at least the same or equivalent information security requirements (see paragraph 7 of Appendix A to Enclosure A, "Individual Functions and Responsibilities") as all DOD authorized users (i.e., military, and DOD government civilian and contract employees) on DOD information systems and networks.

25 March 2003

(1) C/S/As will ensure DOD foreign national employee follows security policies and procedures, and the systems security officer is given authority to enforce policies and procedures.

(2) Prior to access to the system, a foreign national will sign a user agreement (see paragraph 7 of Appendix A to Enclosure A, "Individual Functions and Responsibilities") that includes:

(a) Acknowledging information and information system security policies, procedures, and responsibilities.

(b) Consequences of not adhering to security procedures and responsibilities.

(c) For E-mail accounts, the user name will include individual's nationality (see subparagraphs 5(a)(7) and 5(a)(8) above) to preclude inadvertent disclosure of controlled unclassified information not authorized to foreign nationals (see subparagraph 2b above).

#### 8. DOD Foreign National Contractors

a. Access to DOD-owned or DOD-managed information systems and networks are authorized for controlled unclassified information systems on a need-to-know basis for the contractor's (Non US citizen) official duties.

b. Contractors (Non US citizens) with access to DOD-owned or DOD-managed information systems or networks will comply with the requirements of DOD 5200.2-R (reference 1).

c. Foreign national contractors (Non US citizens) will meet the same information security requirements (see paragraph 7 of Appendix A to Enclosure A, "Individual Functions and Responsibilities") as all DOD users (i.e., military, DOD government civilian and contract employees) on DOD information systems and networks.

(1) C/S/As will ensure foreign national contractor follows security policies and procedures, and the systems security officer is given authority to enforce policies and procedures.

(2) Prior to access to a system, the foreign national contractor will sign a user agreement that includes:

25 March 2003

(a) Acknowledging information and information system security policies, procedures, and responsibilities.

(b) Consequences of not adhering to security procedures and responsibilities.

(c) For E-mail accounts, the user name will include individual's nationality (see subparagraph 5(a)(7) above) to preclude inadvertent disclosure of controlled unclassified information not authorized to foreign nationals (see subparagraph 2b above) and also identify the user as a contractor (e.g., john.smith.ctr.uk@army.mil).

d. A data item description for meeting security requirements in DOD 5200.2-R (reference a) will be included in contracts. It is important to note that the requirement to categorize IT positions in accordance with DOD 5200.2-R (reference a) applies to all positions requiring access to DOD information systems and networks, whether occupied by military, DOD government civilians, or contractors.

#### 9. Foreign National in IT Position

a. All DOD employees and DOD contractors must meet the personnel security and suitability requirements of DOD 5200.2-R (reference a).

b. Only US citizens can fill IT positions (e.g., system administrators) on US-only **classified** systems or networks (e.g., classified enclave connected to SIPRNET, JWICS, or GCCS).

c. When foreign nationals (Non US citizens) are proposed to fill IT positions on DOD **unclassified** information systems, those positions must be categorized and meet investigative requirements, conditions, and controls of DOD 5200.2-R (reference a) and DODI 8500.2 (reference w).

d. Non-US citizens currently performing system or network administration, or other IT positions that do not meet personnel security and suitability requirements, will be phased out, transferred, or released as appropriate in accordance with DOD guidance and personnel regulations and/or applicable international agreements.

#### 10. Release of USG INFOSEC Products or Associated INFOSEC Information to Foreign Governments

a. The Committee on National Security Systems (CNSS), formerly the National Security Telecommunications Information Systems Security

25 March 2003

Committee (NSTISSC), will consider requests to release INFOSEC products or associated INFOSEC information to a foreign government or an international organization if satisfied by requirements identified by DOD components to:

- (1) Protect US national security information that is provided to, or exchanged with, a foreign government or international organization.
- (2) Enhance the objectives and effectiveness of mutual US defense arrangements or coalition operations by providing a means for achieving secure communications interoperability when exchanging military-planning information, or conducting combined or coalition operations that involve US military forces and the military forces of a foreign government(s) or international organization.
- (3) Protect US national security information, which is provided to or exchanged with a foreign government or international organization in support of US efforts to combat the transnational threats of international crime, international terrorism, international drug trafficking, or proliferation of WMD.

b. Requests for release of USG INFOSEC products or associated INFOSEC information must:

- (1) Be consistent with US foreign policy and military or economic objectives.
- (2) Have no unacceptable impact on US signals intelligence (SIGINT) activities.
- (3) Have no adverse impact on the overall INFOSEC posture of the US Government.

c. In cases where the terms of a CNSS release authorization must be documented in a formal memorandum of understanding (MOU), the CNSS may provide negotiating guidelines for the sponsoring department or agency. Prior to signing, the MOU must be reviewed and approved by the DIRNSA, acting as the national manager for national security telecommunications and information systems security to ensure compliance with CNSS release guidelines.

d. Provided the criteria in subparagraphs 9b and 9c above are satisfied, the following limitations apply to the release of INFOSEC products or associated INFOSEC information:



25 March 2003

(1) USG INFOSEC products or associated INFOSEC information will normally not be authorized for release solely for improving the INFOSEC posture of a foreign government or international organization.

(2) The inclusion of INFOSEC products or associated INFOSEC information in weapons, communications, or other major defense systems to provide a complete package for foreign military sales (FMS) or initiatives to promote international competition for system procurements, are not, in and by themselves, acceptable justification for seeking release of those products or information.

(3) The transfer of USG INFOSEC products or associated INFOSEC information will normally be accomplished on a government-to-government basis through FMS channels. Use of other than FMS channels, such as providing INFOSEC products, information, or services as part of arrangements with foreign countries for cryptologic support pursuant to 10 USC 421 (reference jj), will be considered and approved on a case-by-case basis by the national manager. As necessary, training will be provided to the recipients of USG INFOSEC products or associated INFOSEC information to ensure proper operation and protection in accordance with prescribed USG standards.

e. Requests for the release of INFOSEC products or associated INFOSEC information to foreign governments and international organizations will be processed as follows in accordance with National Security Telecommunications and Information Systems Security Procedure (NSTISSP) No. 8 (reference kk).

(1) Components desiring to release INFOSEC products or associated INFOSEC information will make an initial determination that the proposed release satisfies the criteria of NSTISSP No. 8 (reference kk).

(2) Requests satisfying the criteria will be submitted to the national manager (DIRNSA) through the C/S/A to determine how the requirement can best be satisfied, as well as assessing whether the proposed release would impact adversely on US SIGINT or INFOSEC equities.

(3) In cases where a releasability decision falls within the purview of the authorities assigned by NSTISSP No. 8 (reference kk), the national manager may recommend and approve the release of the INFOSEC products or associated INFOSEC information that will satisfy the stated requirement.

(4) For other cases, the national manager will provide feedback to the requesting department or agency on a recommended INFOSEC solution. Based on the feedback, the requesting department or agency will determine resource availability and identify a proposed method of transfer (e.g., sale, lease, or

25 March 2003

loan). If resources are unavailable, the requesting department or agency will work with the national manager to address shortfalls.

(5) The national manager will refer requests requiring a release determination by the full CNSS membership to the CNSS chairman through the CNSS secretariat. The national manager will include the following in the referral:

- (a) Comments regarding the most appropriate INFOSEC solution.
- (b) A recommendation regarding the most acceptable means of transfer.
- (c) A SIGINT and INFOSEC assessment.
- (d) A recommended CNSS action.

(6) In implementing release decisions of the CNSS, the requesting C/S/A will coordinate the provision of the appropriate INFOSEC products or associated INFOSEC information with the national manager and provide details, within 30 days of the date of actual transfer, regarding the quantities of materials involved and method of transfer.

(7) Appeals on a CNSS decision regarding release can be made to the Secretary of Defense.

f. The disclosure or release of US COMSEC information to foreign governments or international organizations will be done only when determined to be in the best interest of the US Government and in accordance with NSTISSP No. 8 (reference kk) and DODI 5225.1 (reference ll). Procedures for determining responses to release requests (see Appendix G, Annex C, "Communications Security") require consideration of risks resulting from disclosure or release outlined in CJCSI 6510.06 (reference mm).

## APPENDIX C TO ENCLOSURE C

## ELECTRONIC NOTICE AND CONSENT BANNER

1. All DOD information systems (to include routers and servers) must display a "log-on notice and consent banner" (Figure C-C-1) that presents the notice information on the initial log-on page regardless of access methodology (e.g., network, website, remote access, dial-in, etc.). The requirement to display the banner before login can be met on most devices, but these devices (including router) cannot audit the keystroke to meet an auditable event requirement. The log-on notice and consent banner, as a minimum, must advise users of the following:

- a. The system is a DOD system.
- b. The system is subject to monitoring.

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED US GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Figure C-C-1. Example of a Notice and Consent Banner

C-C-1

Appendix C  
Enclosure C

**FOR OFFICIAL USE ONLY**

c. Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.

d. Use of the system constitutes consent to monitoring.

e. This system is for authorized US government use only.

2. New information systems (to include servers and routers) must include a log-on banner when they are put into service.

3. System owners will periodically review their existing electronic banners to ensure compliance with DOD policy in consultation with appropriate legal counsel.

4. The following measures will be utilized with the electronic banner to distribute notification and ensure user awareness.

a. Notice and consent decals placed on information systems.

b. Notice in the daily bulletins or similar media.

c. Notices to all users advising them of the monitoring program.

d. A statement in SOPs, similar publications, or user agreements that "system use" constitutes consent to monitoring.

e. New personnel notified of this policy during initial processing.

f. Periodic security awareness briefings for all users.

5. The warning banner will be displayed after a successful log-on and will remain displayed on the user's screen until a keystroke is entered. This serves as an auditable event that the banner could be read.

## APPENDIX D TO ENCLOSURE C

## PHYSICAL AND ENVIRONMENTAL SECURITY

1. Description. Physical security of information systems is as vital as protecting against unauthorized electronic activity.

a. The physical security program is defined as that part of security concerned with active and passive measures designed to prevent unauthorized physical access to personnel, equipment, installations, materiel and documents, and to safeguard them against espionage, sabotage, damage, and theft.

b. The procedures suggested here for developing and implementing a physical security program include:

(1) Analyze the risk as the basis for development of a security policy.

(2) Select and implement appropriate security measures to reduce exposure to losses.

(3) Develop contingency plans for backup operation, disaster recovery, and emergencies.

(4) Provide indoctrination and standardized training for all personnel accessing the system.

(5) Plan and conduct continuing tests and inspections and adjust security measures and contingency plans as needed.

c. Physical security is a primary command responsibility.

d. DOD components will have each commander of a major command ensure that the physical security plan developed includes information systems or facilities under their command.

(1) The information system portion of the plan may be an annex to an existing host installation security plan.

(2) Only the applicable parts of the total plan will be distributed to personnel at the facility.

2. Physical Security Programs. Physical security programs provide the means to counter unauthorized physical access by people during peacetime, crisis, and in conflict to DOD facilities and information systems. Organizations or people that pose potential physical security threats include:

- a. Foreign intelligence services.
- b. Paramilitary forces.
- c. Terrorists and saboteurs.
- d. Criminals.
- e. Protest groups.
- f. Disgruntled employees.
- g. Cleaning service personnel who are members or work for one of the threat groups identified above.

3. Physical Security Planning

- a. The following must be utilized in the planning of physical security:
  - (1) Use electronic security systems to reduce both threats and vulnerabilities and reliance on fixed security forces.
  - (2) Integrate physical security into contingency, mobilization, and wartime plans, and test these procedures and measures during the exercise of these plans.
  - (3) Coordinate with installation operations security, crime prevention, IA, information system security, personnel security, COMSEC, and physical security programs to provide an integrated and coherent effort.
  - (4) Implement on-site tactical defense and penetration training for local security forces.
  - (5) Create and sustain physical security awareness.
  - (6) Identify resource requirements to apply adequate measures.
  - (7) Implement physical security measures, which are a combination of active or passive systems, devices, and personnel used to protect information

systems or facilities that house information systems from possible physical threats and provide physical access control. Physical access controls include:

(a) Restrict the entry and exit of personnel, equipment, and media from an area, such as a building, data center, or room containing a LAN server.

(b) Restrict access to areas containing system hardware and locations of system wiring, fiber optics, etc. Review and update contingency plans for supporting services (such as electric power), backup media, and any other elements required for the system's operation.

(8) Review physical access controls in each area -- both during normal duty hours and at other times -- particularly when an area may not be occupied.

b. Security measures may include, as appropriate:

(1) Security forces and owner or user personnel.

(2) Military working dogs.

(3) Physical barriers, facility hardening, and use of active delay or denial systems.

(4) Secure locking systems, containers, and vaults.

(5) IDSs against physical entry.

(6) Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).

(7) Protective lighting.

(8) Badging systems, access control devices, materiel or asset tagging systems, and contraband-detection equipment.

4. Security System Level and Mission Category. Figure C-D-1 provides a matrix comparing security system levels to information systems mission category when developing a physical security plan. The mission reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighter's combat mission.

25 March 2003

Security System Level	Mission Assurance Category
<p><b>A</b></p> <p>Integrated electronic security systems, entry and circulation control, barrier systems, access delay and denial systems, dedicated security forces, designated immediate response forces</p>	<p><u>MAC I:</u></p> <p>Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.</p>
<p><b>B</b></p> <p>Electronic security systems, entry and circulation control, barrier systems, dedicated security forces, designated response forces</p>	<p><u>MAC II:</u></p> <p>Systems handling information that is important to the support of deployed and contingency forces. The information must be accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).</p>
<p><b>C</b></p> <p>Electronic security systems, entry and circulation control, barriers, security patrols, designated response forces</p>	<p><u>MAC III:</u></p> <p>Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information)</p>

Figure C-D-1. Security System Level and Mission Category

a. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each information system location or facility.

b. The physical security program will be tailored to that particular information system(s) and the facility where the information system(s) is located.

c. Controlling access to areas containing vital physical components of information systems must be addressed. Facilities may be designated and posted as restricted areas.

5. Fire Safety Factors. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and widespread damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an



entire building. Consequently, it is important to evaluate the fire safety of buildings that house information systems.

#### 6. Failure of Supporting Infrastructure

a. Systems and the people who operate them need to have a controlled operating environment. Failures of electric power, heating and air-conditioning systems, water, sewage, and other critical infrastructure will usually cause a service interruption and may damage hardware. Organizations will ensure that these critical utilities, including their many elements, function properly and contingency plans are developed and exercised.

b. Installing whole-building protection will preclude installation of dozens if not hundreds of smaller pieces of equipment throughout the entire building and/or organization. Some ways to protect against mission failure when the supporting infrastructure fails include

(1) Use protected power sources and/or uninterruptible power supplies to ensure operation of critical computer systems, routers, and firewalls.

(2) Use conditioned power sources and/or surge protectors to prevent or limit damage from spikes, surges, and lightening strikes.

7. Plumbing Leaks. Plumbing leaks can be seriously disruptive. An organization will ensure the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shut-off valves) are known.

(INTENTIONALLY BLANK)

## APPENDIX E TO ENCLOSURE C

HANDLING, MARKING, AND LABELING INFORMATION AND  
THE PROTECTION OF CLASSIFIED AND UNCLASSIFIED NATIONAL  
SECURITY-RELATED INFORMATION

1. Handling, Marking, and Labeling Information. See DOD 5200.1-R (reference i) for additional guidance.

a. Classified Information

(1) Classified information must be properly marked and safeguarded so that only authorized persons have access; it is used only for its intended purpose and retains content integrity.

(2) National security systems (see Glossary), including those operated and maintained by USG contractors, must be protected to prevent unauthorized access, DOS, compromise, tampering, or exploitation of information.

(3) Authorized products and services (NSA-endorsed) and/or certified and accredited systems must be used to protect national security telecommunications and information systems in accordance with DODD C-5200.5 (reference nn).

(4) DODI S-3600.2 (reference u) provides classification guidance for information operations.

(5) Live connections to the SIPRNET are considered classified at the SECRET level. These connections will be provided with safeguards IAW DOD 5200.1-R (reference i)

b. Controlled Unclassified Information

(1) Controlled unclassified information must be properly marked FOUO (or other authorized caveat such as "Limited Distribution") and safeguarded so that only authorized persons have access; it is used only for its intended purpose and retains content integrity.

(2) Sensitive information subject to Public Law 100-235 (reference oo) will be protected during transmission, processing, and storage by products validated as meeting applicable federal information processing standards or by NSA-endorsed COMSEC products, techniques, and protected services.

c. Unclassified Information

(1) Unclassified information transmitted by and between US military forces and contractors will be protected against tampering, loss, and destruction commensurate with the associated risk of its exploitation.

(2) Except in prescribed instances, military forces may procure and use commercial cryptographic equipment and techniques to satisfy communications protection requirements for unclassified information (National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) INFOSEC/1-00 reference pp). NSA-approved equipment must be used if the function, operation, or use of the equipment involves the C2 of military forces or is critical to the direct fulfillment of military intelligence missions.

(3) Suggested safeguards for unclassified information are outlined in Office of Management and Budget (OMB) Circular No. A-130 (reference qq) and include applicable personnel, physical, administrative, and technical controls.

d. Storage Media

(1) Information storage media used in a classified information system is classified at the level of that information system. Information storage media will have external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. IAOs and SAs will identify the removable storage media to be used with a system.

(2) Removable media will be marked, physically controlled, and safeguarded in the manner prescribed for the highest classification level ever recorded on it until destroyed or processed in accordance with DOD 5200.1-R (reference i).

(3) Nonremovable information storage media will bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. If it is difficult to mark the nonremovable media itself, the labels described above may be placed in a readily visible position on the cabinet enclosing the media.

e. Marking Hardware Components. Procedures will be implemented to ensure that all components of an information system, including input/output devices that retain information, terminals, stand-alone microprocessors, and

25 March 2003

word processors used as terminals, bear a conspicuous, external label. This label will state the highest classification level and most restrictive classification category of the information accessible to the component in the information system.

f. Marking Human-Readable Output. Human-readable output will be marked appropriately, on each human-readable page, screen, or equivalent (e.g., the proper classification must appear on each page of classified printouts).

## 2. Protecting Unclassified National Security-Related Telecommunications Information

a. Table C-E-1 is a guideline only. Omission of a particular information category or type does not preclude a separate determination that such information is valuable to an adversary. C/S/As are encouraged to establish additional guidelines to suit their particular needs.

b. DODD C-5200-5 (reference nn) requires all sensitive (national security-related) information to be protected commensurate with associated exploitation risks. DOD and agency heads are responsible for deciding which of their transmittable unclassified information is sensitive (national security-related). This appendix provides guidelines for identifying information systems or communications containing unclassified national security-related information in this category.

c. Information disclosure to US adversaries through exploitation of the Nation's unprotected information systems poses a serious threat to US national security. The need to protect information requires participation among the Department of Defense, government agencies, and the private sector. Information sent between government agencies and their contractors, between government contractors, or between government contractors and their subcontractors must be protected. Whenever information has value and can be intercepted, it should be expected that attempts would be made to exploit it. Generally, if the government department, agency, contractor, or subcontractors believe the information will be useful to an adversary, it should be protected.

d. These guidelines apply only while information is being electronically transmitted. If this information is not protected during transmission, it is vulnerable to interception and exploitation. The guidelines in this appendix identify kinds of information for which intercept would be contrary to the national interest.

e. The guidelines provide a sample of specific categories and types of information considered to be sensitive (national security-related). Relative values of each information type are on a six-point scale, with "1" being the highest. These values generally describe expected benefits of protection and a suggested priority for safeguarding this information.

f. Information types with assigned values of 1, 2, or 3 should be presumed to require protection whenever an exploitation risk is present. Values 4, 5, or 6 may also require protection when an exploitation risk is present, depending on the timeliness of the information, its quantity, or other characteristics. A case-by-case evaluation may be appropriate in such circumstances. See Appendix H to Enclosure C, "Protection Mechanisms – Levels of Concern and Robustness," for more information on protection mechanisms.

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	1. <u>Military</u>
1	a. <u>Force Planning</u> . Unclassified information on doctrine, concepts, and plans for employing strategic and general-purpose forces; national strategic targeting philosophies and doctrine for nuclear weapon employment, stockpile maintenance; national appraisal of opposing capabilities and vulnerabilities; national C2 systems, their strengths and vulnerabilities; military production and procurement, level and composition of military expenditures, including changes in funding levels for the military sector for major components of military spending, military research, development, test and evaluation (RDT&E) expenditures.
1	b. <u>Strategic Offensive Forces</u> . Unclassified information on nonspecific capabilities of the intercontinental ballistic missile force, ballistic and cruise missile submarine forces, intermediate and medium-range ballistic missile forces, strategic doctrine, general capabilities for use of space vehicles in a nuclear offensive role; and general characteristics of strategic offensive weapons systems.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information

25 March 2003

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
1	c. <u>Strategic Defense Forces</u> . Unclassified information on nonspecific capabilities of the ballistic missile defense force, fighter/interceptor defense force, surface-to-air missile force, antisubmarine warfare forces, strategic doctrine, intelligence-collection systems, equipment, and facilities; general capabilities for attack against space satellites; nuclear explosion assessment system; RDT&E on strategic defense weapon systems; and research and development related to development of directed energy.
2	d. <u>Armed Conflict, Hostilities Indications, and Warning</u> . Unclassified information on indications of preparation for or initiation of an attack.
2	e. <u>General-Purpose Forces</u> . Unclassified information on capabilities and vulnerabilities of ground forces, naval forces, air transport forces, and tactical air forces, including strength, organization disposition, C2, tactical doctrine, operating practices, training levels, mobility, support systems availability, equipment and facilities; biological and chemical warfare doctrine and concepts; capabilities and vulnerabilities of paramilitary forces such as border guards, national policy forces, and internal security forces, RDT&E on and characteristics of general purpose systems.
2	f. <u>Support Capabilities and Military Environment</u> . Unclassified information on general capabilities of Service components to render services required by military forces to execute assigned missions; influence of country's physical environment on capabilities, dispositions, or mobility of military forces; existence of plans and programs to limit casualties and damage to counter value targets by civil defense or other passive means, general capabilities to support military forces in combat, training and readiness of Reserve Forces, mobilization system and time-phased capabilities of the mobilization program; concepts, doctrine, strategy, and tactics and capabilities for using electronic warfare; RDT&E on and characteristics of military electronics systems.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

25 March 2003

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	1. <u>Military</u> (cont'd)
3	g. <u>Arms Transfer, Military Assistance, and Out-of-Country Deployments</u> . Unclassified information on provision and/or acceptance of arms and military assistance, including transfers, negotiations and contracts, sales, loans, and/or grants, and deliveries of military and military-related equipment, services, and/or military training; national plans, capabilities, and actions to deploy forces and associated weapons to foreign countries, in international waters, in airspace or outer space, including the purposes and priority attached to deployment to particular countries or areas.
	2. <u>Political</u>
1	a. <u>Attitudes and Actions toward Arms Control, Force Limitations, Cease-Fire and/or Peace Agreements</u> . Unclassified information on national attitudes, actions, and compliance concerning arms limitations proposals; politico-military assessment of related risks and limitations of arms control, force level agreements, cease-fire or peace treaties; policy objectives and actions regarding strategic and regional arms control and disarmament.
1	b. <u>Intelligence and Security Services</u> . Unclassified information on effort to deceive, neutralize, or interfere with foreign target technical intelligence collection capabilities; structure, capabilities, and effectiveness of positive intelligence and counterintelligence (CI) organizations internal security effectiveness; subversion techniques; national capabilities to conduct psychological warfare operations; capabilities and programs for sabotage directed against personnel, programs, and facilities of other nations.
2	c. <u>US Foreign Relations with Developing Countries</u> . Unclassified information on national foreign policy intentions, objectives, programs, negotiating positions, and actions.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)



25 March 2003

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	2. <u>Political</u> (cont'd)
2	d. <u>US National Security Objectives</u> . Unclassified information on national objectives for development of a security posture vis-à-vis potentially hostile nations; policies, intentions, programs, and actions favoring or inhibiting active participation in military alignments or alliances, including the receipt and/or provision of military support.
3	e. <u>US Foreign Relations with Allies</u> . Unclassified information on national foreign policy intentions, objectives, negotiating positions, and actions.
3	f. <u>US Participation in Multilateral Organizations</u> . Unclassified information on national policy objectives, programs, negotiating positions, and actions likely to support or conflict with political and economic interests of other nations as they relate to the functioning and activities of international organizations of all types (e.g., the United Nations and its organizations) except military alliances.
4	g. <u>Resource and Environmental Issues</u> . Unclassified information on national interest in and actions to deal with environmental problems, especially atmospheric and water pollution; to regulate exploitation of polar, ocean, and seabed resources; and to promote favorable action on law-of-the-sea issues.
4	h. <u>Internal Political Affairs</u> . Unclassified information on domestic policy objectives, programs, and actions; internal political developments; changes in the representation and roles of politically significant parties and factions; key influences on the internal decision-making process; government capability to identify and deter and/or suppress elements fostering insurgency.
4	i. <u>US Political Biographic Data</u> . Unclassified information on background, associations, actions, medical, and psychological data on essential political figures. Personality data on key figures to include leadership style, decision making, attitudes, worldviews, crisis reaction, and negotiating behavior.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	2. <u>Political</u> (cont'd)
5	j. <u>Transit Rights, Authorizations, and Facilities Arrangements</u> . Unclassified information on national attitudes and actions regarding the granting of transit rights, authorizations, and facilities arrangements.
	3. <u>Economic</u>
2	a. <u>Technology Transfer</u> . Unclassified information on attitudes and policies toward technology transfer; compliance with international strategic trade controls.
2	b. <u>Telecommunication Services</u> . Unclassified information on the capabilities and location of civilian and military telecommunications equipment and facilities, including landline (wire and cable), radio (troposcatter, radio relay, and satellite systems), telephone, teleprinter, facsimile, data transmission, television, and other services.
3	c. <u>Energy Resources and Policies</u> . Unclassified information on capacity to produce and access oil, coal, nuclear, and other energy resources; plans and policies for exploitation and marketing, conservation and control of use; stockpiling, export and import; policies on pricing and participation in multilateral efforts affecting supply, including forecasts of energy demand.
3	d. <u>Agricultural Policies, Food Supplies, and Mineral Resources</u> . Capacity to produce and access to food and foodstuffs; impact on population of marketing, stockpiling, and control of food products and fisheries; capacity to produce and access to minerals and mineral products; plans, policies, and activities affecting access to resources, including producers' consumer marketing arrangements.
4	e. <u>Monetary and Financial Developments</u> . Unclassified information on fiscal and monetary policies and objectives; national budgets and financing of national debt; balance-of-payment objectives, including exchange-rate policy; gold prices and transactions; international monetary proposals.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

25 March 2003

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	3. <u>Economic</u> (cont'd)
4	f. <u>Business Activities and Conditions</u> . Unclassified information on commercial and financial developments; business conditions, sales opportunities for US manufacturers and industrial products; sales opportunities for investment and investment climate; investment activities at home and abroad; government procurement activities; and changes in trading policies that affect export opportunities for US producers.
4	g. <u>Activities of Multinational Corporations</u> . Unclassified information on activities of foreign multinational corporations as they affect economic relations between the United States and subject country, including specific inward and outward foreign investment deals; technology transfer; the amount of production, foreign trade, and sales attributable to foreign subsidiaries of US firms.
4	h. <u>Foreign Economic Relations with Advanced Countries</u> . Unclassified information on foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.
4	i. <u>Foreign Economic Relations with Other Countries</u> . Unclassified information on foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.
5	j. <u>Economic Growth and Stability</u> . Unclassified information on changes in leading economic indicators; economic policy responses to such internal and external changes in economic performance, and the likely effects of these responses.
5	k. <u>Industrial Production</u> . Unclassified information on capacity to produce basic, intermediate, and final industrial goods needed for civilian and military use; prospective evolution of the industrial sector.
5	l. <u>International Trade Trends</u> . Unclassified information on value, tonnage, and commodity composition of exports and imports, especially changes in market shares; disparities between export and domestic prices of export goods, and transportation bottlenecks in foreign trade.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	3. <u>Economic</u> (cont'd)
5	m. <u>Trade and Transport Policies and Negotiating Positions</u> . Unclassified information on trade liberalization, tariff and nontariff barriers, other restrictions, proposed commodity agreements, export credit policies and policies regarding trade in major crops; plans and policies related to commercial air or maritime activities.
5	n. <u>Advanced Industrial and Manufacturing Processes and Products</u> . Unclassified information on new investment and application of funds (including extent of government subsidy) and other resources to the research, development, testing, and application of new, advanced industrial and manufacturing processes and products, and the introduction or manufacture of significant new products.
5	o. <u>Foreign Economic Relations with Communist Countries</u> . Unclassified information on foreign economic policies and programs; granting or extension of foreign loans and grants for nonmilitary purposes.
5	p. <u>Transportation Systems</u> . Unclassified information on the operational capabilities, vulnerabilities, and limitations of transportation networks and facilities (railways, highways, airlines, waterways, pipelines, transshipment areas, warehouses, airfields, ports, and harbors), to include their use by military forces for movement of supplies and reinforcements; capabilities, disposition, and employment of merchant fleet.
	4. <u>Special Subjects</u>
1	a. <u>Other Government Information</u> . Unclassified information provided to the United States by a foreign government or international organization, or produced by the United States under an arrangement with such entity, with expectation or condition that the information will be private.
1	b. <u>Other-Agency Information</u> . Unclassified information provided to the Department of Defense by another US department or agency with the expectation or condition that the information will be protected within the Department of Defense.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

<u>INFORMATION VALUE GUIDE FOR PROTECTING UNCLASSIFIED NATIONAL SECURITY-RELATED TELECOMMUNICATIONS INFORMATION</u>	
<u>VALUE</u>	<u>CATEGORY</u>
	4. <u>Special Subjects (cont'd)</u>
1	c. <u>Weapons of Mass Destruction</u> . Unclassified information on WMD proliferation including nuclear, chemical, and biological devices, infrastructure, C2 systems, delivery systems, acquisition programs, the decision by nation states, subnational groups or terrorist organizations to pursue WMD technology including research and development facilities, special nuclear materials, precursor chemicals, actions of source countries or organizations. Transportation and safeguards.
2	d. <u>Technology</u> . Unclassified information on any design, manufacturing, and related technical data concerning critical arrays of know-how identified on the DOD military critical technologies list.
5	e. <u>National Science Policies and Programs</u> . Unclassified information on the administration of and organization of science and technology work in the governmental, industrial, and academic sectors.
5	f. <u>Human Rights</u> . Unclassified information on attitudes and actions toward human rights.
6	g. <u>Illicit Drug Traffic</u> . Unclassified information on cultivation, production, processing, storage, transportation, and distribution of illicit narcotics and dangerous drugs; related economic and financial transactions, including money laundering and recycling; activities of nongovernmental organizations, including criminal enterprises and groups, engaged in these activities.

Table C-E-1. Information Guide for Protecting Unclassified National Security-Related Telecommunications Information (cont'd)

(INTENTIONALLY BLANK)

## APPENDIX F TO ENCLOSURE C

## DEFENDING BACKBONE NETWORKS

1. Backbone Networks. To accomplish defending the network objectives for backbone networks, the security requirements described below will be implemented.

2. Access Control

a. Access controls must be used to differentiate user's access to the network devices. For example, access controls must enforce user's access to status information vs. configuration information.

b. Access controls must limit access to the network management center.

3. Authentication

a. Network devices must authenticate the source of all configuration changes from other network devices, such as routing messages.

b. Whenever possible, network devices must strongly authenticate all connection requests from network management personnel.

c. Network management systems must authenticate network management personnel prior to granting access.

d. The network management center must authenticate the source of all communications entering the network management center from external networks.

e. The network management center must provide strong protection of dial-up access and authenticate all dial-in remote-access users prior to granting them access to the network management center.

4. Confidentiality

a. The confidentiality of key material must be protected.

b. The network management system will provide confidentiality of routing information, signaling information, and network management traffic to provide traffic-flow security.

c. Confidentiality of data-in-transit over backbone networks must be maintained using appropriate encryption measures as per the classification or sensitivity level of the data.

5. Integrity. Safeguards will be in place to detect and minimize inadvertent modification or destruction of data. All internal DOD electronic transactions should be provided data integrity and authentication by the appropriate combination of digital signature, keyed hash, and encryption mechanisms. The integrity of the following must be protected:

- a. Communications between network devices.
- b. Hardware and software in network devices.
- c. Communications between network devices and the network management center.
- d. Vendor-supplied hardware and software.
- e. Dial-in communications to the network management center.

6. Nonrepudiation

- a. Network personnel must not be able to repudiate changes to the configuration of network devices (if possible).
- b. Vendors must not be able to repudiate vendor-supplied or developed hardware or software (if possible).



25 March 2003

## APPENDIX G TO ENCLOSURE C

## COMMUNICATIONS SECURITY

1. COMSEC Material Control System. USG policy is to encourage COMSEC material and technique use and to safeguard COMSEC materials assuring continued integrity, prevention of unauthorized access, and controlling the spread of COMSEC materials, techniques, and technology when not in the best interest of the United States and its allies (NCSC-1 (reference rr)). Implementation of this policy requires each department and agency holding COMSEC keying material establish a COMSEC material control system (CMCS) into which all COMSEC keying material will be placed. Other COMSEC material may be placed in the CMCS or any other material control system providing the requisite security and management control.
2. Granting Access to US Classified Cryptographic Information. Certain US classified cryptographic information requires special access controls. Access to this information must only be granted to individuals satisfying specific criteria. See Annex A of this appendix, "Cryptographic Access Criteria."
3. Release of COMSEC Information to US Nongovernmental Sources. The USG will normally conduct COMSEC operations. Military forces may obtain required COMSEC support from, and may provide COMSEC information and material to, US nongovernmental sources within limitations outlined in NCSC-2 (reference ss) and Annex B of this appendix, "Release of COMSEC Information to US Contractors and Other US Nongovernmental Organizations and Persons."
4. Disclosure or Release of COMSEC Information to Foreign Governments and International Organizations. The disclosure or release of US COMSEC information to foreign governments or international organizations will be done only when determined to be in the best interest of the USG and in accordance with NSTISSP No. 8 (reference kk), CJCSI 6510.06 (reference mm), and CJCSI 5221.01 (reference dd). Procedures for determining responses to release requests can be found in Annex C of this appendix, "Disclosure or Release of COMSEC Information to Foreign Governments and International Organizations." This appendix requires consideration of risks resulting from disclosure or release.
5. COMSEC Monitoring. USG agencies and departments conduct COMSEC-monitoring activities only as necessary to determine the degree of security provided to government information systems and telecommunications and aid in countering their vulnerability. Government information and telecommunications are subject to COMSEC monitoring by duly authorized

25 March 2003

government entities (as specified by individual department or agency regulations). Users of these systems must be properly notified in advance, in accordance with guidelines in Annex D of this appendix, "COMSEC Monitoring," DODD 4640.6 (reference tt), and NSTISSD No. 600 (reference uu).

## ANNEX A TO APPENDIX G TO ENCLOSURE C

## CRYPTOGRAPHIC ACCESS CRITERIA

1. Access Requirements

a. An individual may be granted access to US classified cryptographic information only if that individual meets the following NSTISSP No. 3 (reference vv) criteria:

(1) Is a US citizen.

(2) Is an employee of the USG, USG-cleared contractor or contractor employee, or is employed as a USG representative (including consultants of the USG).

(3) Possesses a security clearance appropriate to the classification of the US cryptographic information to be accessed.

(4) Possesses a validated need to know.

(5) Receives a security briefing appropriate to the classified cryptographic information to be accessed.

(6) Acknowledges access by signing a cryptographic access certificate.

b. When department or agency heads so direct, an individual granted access in accordance with this policy may be required to acknowledge the possibility of being subject to a nonlifestyle, CI scope polygraph examination administered in accordance with department or agency directives and applicable law.

c. All persons indoctrinated for cryptographic access may be subject to special requirements prescribed in their respective department or agency security directives, regarding unofficial foreign travel or contacts with foreign nationals.

2. Procedures. These procedures apply to all individuals satisfying the requirements of paragraph 1 and whose official duties require continuing access to US classified cryptographic information. These procedures apply to individuals assigned:

a. As COMSEC custodians or alternates.

C-G-A-1

Annex A  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

- b. As producers or developers of cryptographic keys or logic.
- c. As cryptographic maintenance or installation technicians.
- d. To spaces where cryptographic keying materials are generated or stored.
- e. To prepare, authenticate, or decode valid or exercise nuclear control orders.
- f. In secure telecommunications facilities located in fixed ground facilities or on board ships.
- g. Any other responsibility with access to US classified cryptographic information that is specifically identified by the head of a department or agency.

3. Exceptions. To meet urgent operational needs, department or agency heads may approve exceptions to these procedures. Records of exceptions granted will be made available on request from the national manager for telecommunications and INFOSEC.

#### 4. Sample Cryptographic Access Briefing

a. You have been selected to perform duties requiring access to US classified cryptographic information. It is essential that you are aware of facts relevant to information protection before access is granted. You must know the reason why special safeguards are required to protect US classified cryptographic information. You must understand the directives requiring safeguards and penalties you incur for unauthorized disclosure, retention, or negligent handling of information. Failure to properly safeguard information could cause serious damage or irreparable injury to US national security.

b. US classified cryptographic information is especially sensitive because it is used to protect other classified information. Any piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. Safeguards placed on US classified cryptographic information are a necessary component of government programs to ensure our Nation's vital secrets are not compromised.

25 March 2003

c. Because access to US classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only the cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, department or agency implementing directives covering the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

d. Especially important to the protection of US classified cryptographic information is the timely reporting of any known or suspected information compromise. If a cryptographic system is compromised and the compromise is not reported, continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

e. The following two paragraphs will be included only when the applicable department or agency head directs:

(1) As a condition of access to US classified cryptographic information, you must acknowledge the possibility that you may be subject to a nonlifestyle, CI scope polygraph examination. This examination will be administered in accordance with the provisions of (insert appropriate department or agency directive) and applicable law. This polygraph examination will only encompass questions concerning espionage, sabotage, or questions relating to unauthorized disclosure of classified information.

(2) You have the right to refuse a nonlifestyle, CI scope polygraph examination. Such refusals will not be cause for adverse action but may result in your being denied access to US classified cryptographic information. If you do not at this time wish to sign such an acknowledgment of this provision as a part of executing a cryptographic access certification, this briefing will be terminated, and the briefing administrator will so annotate the cryptographic access certificate.

f. You should know that intelligence services of some foreign governments prize the acquisition of US classified cryptographic information. They will go to extreme lengths to compromise US citizens and force them to divulge cryptographic techniques and materials protecting the Nation's secrets. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to coercion attempts to divulge US classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions revealing your knowledge of, or access

C-G-A-3

Annex A  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

25 March 2003

to, US classified cryptographic information and thus avoid highlighting yourself to those seeking the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding US classified cryptographic information must be reported immediately to (insert appropriate security office).

g. In view of the risks noted above, unofficial travel to certain communist or other designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

h. Finally, you must know that should you willfully or negligently disclose to any unauthorized persons any of the US classified cryptographic information to which you will have access, you will be subject to administrative and civil sanctions, including adverse personnel actions and criminal sanctions under the Uniform Code of Military Justice and/or the appropriate criminal laws of the United States, as appropriate.

C-G-A-4

Annex A  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

25 March 2003

## ANNEX B TO APPENDIX G TO ENCLOSURE C

RELEASE OF COMSEC INFORMATION TO US CONTRACTORS AND OTHER  
US NONGOVERNMENTAL ORGANIZATIONS OR PERSONS

1. General. The government will normally conduct COMSEC operations. Military forces may obtain required COMSEC support from and provide COMSEC information and material to US nongovernmental organizations or persons within the limitations of NCSC-2 (reference ss).
2. Standards and Procedures. Security standards and procedures applicable to COMSEC information release will be consistent with established policies. In particular:
  - a. Individuals granted access to COMSEC information must be US citizens. Access will be controlled on a strict need-to-know basis and granted only in conformance with procedures established for the particular type of COMSEC information involved. Release request for COMSEC information to US residents who are not US citizens will be processed as an exception to policy.
  - b. Contracting for design, development, modification, production, or developmental testing of cryptographic equipment requires the specific approval of DIRNSA.
  - c. As a prior condition of release, COMSEC information provided to US citizens who are not part of the government will be controlled in a manner to prevent its further dissemination or transfer outside the government.
  - d. Individuals requiring access to US COMSEC information must comply with applicable cryptographic access policies.
3. Criteria. COMSEC information may be released when the following criteria are met:
  - a. A valid need must exist for an individual or organization to:
    - (1) Install, maintain, or operate COMSEC equipment for the USG.
    - (2) Participate in the design, planning, production, training, installation, maintenance, operation, logistic support, integration, modification, testing, or study of COMSEC material or techniques.

C-G-B-1

Annex B  
Appendix G  
Enclosure C**FOR OFFICIAL USE ONLY**

(3) Electrically communicate classified national security information in a cryptographically secure manner or unclassified national security-related information by COMSEC-protected means.

b. Individuals granted access to classified COMSEC information must hold a final government security clearance for the classification level involved. Clearances of facility security officers, COMSEC custodians, and alternate COMSEC custodians must be predicated on a current favorable background investigation.

c. Everyone provided access to COMSEC information must be annually briefed regarding the unique nature of COMSEC information and their responsibilities to properly safeguard and control it.

d. All individuals maintaining government COMSEC equipment must receive formal NSA-approved training on such equipment.

4. Responsibilities. DOD components identifying a requirement to release COMSEC information are responsible as follows:

a. Determine that releases are in the best interests of the USG.

b. Maintain records of all organizations and self-employed individuals provided access to USG COMSEC information.

c. Notify NSA of contract awards or other releases of COMSEC information and material. Information provided should include the name of the contractor, licensee, or individual, the subject matter of the contract or provision, and the nature of the COMSEC information released.

d. Ensure performance of contractors or licensees meets established COMSEC standards and doctrine, including standards of security and quality.

e. Incorporate specified access criteria into contracts and other appropriate documents whenever individuals who are not employees of the USG provide services.

5. Exceptions. Exceptions to these procedures may be granted by the CNSS only, except for waivers to physical security standards protecting COMSEC information and material, which may be approved by DIRNSA. Prior approval must be obtained in each case. Requests for CNSS approval, with justification and explanatory details, will be forwarded to the CNSS through DIRNSA. The following checklist (Figure C-G-B-1) should be used as a guideline.

C-G-B-2

Annex B  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**



**CHECKLIST FOR PREPARING EXCEPTIONS REQUESTS  
TO THE PROVISIONS OF NCSC-2**

1. Identify the individual and/or organization, their citizenship, their level of security clearance, and the location(s) at which COMSEC functions will be performed.
2. Identify the COMSEC functions the nongovernmental organization or individual will perform; the COMSEC information and/or material to which the individual(s) will have access; the number of personnel involved; their training certification and any training required.
3. List the classification of the COMSEC information to which personnel will have access.
4. Indicate whether personnel will be using keying materials marked "CRYPTO," which are held or used by government departments and agencies. If so, has consideration been given to providing unique operational keying materials?
5. Indicate what additional administrative and/or security measures will be implemented.
6. Identify the inclusive dates personnel will have access to COMSEC information under the contract or arrangement provisions.
7. Identify the government department or agency responsible for assuring the security of nongovernment COMSEC operations and/or functions.
8. Identify the specific provision of NCSC-2 (reference ss) for which an exception is required.

Figure C-G-B-1. Checklist for Preparing Exception Requests

(INTENTIONALLY BLANK)

C-G-B-4

Annex B  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

## ANNEX C TO APPENDIX G TO ENCLOSURE C

DISCLOSURE OR RELEASE OF COMSEC INFORMATION TO FOREIGN  
GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS

1. General. The disclosure or release of US COMSEC information to foreign governments or international organizations will be done only when determined to be in the best interest of the USG and in accordance with NSTISSP No. 8 (reference kk), CJCSI 6510.06 (reference mm), and CJCSI 5221.01 (reference dd). Procedures for determining responses to release requests can be found in Enclosure B of CJCSI 6510.06 (reference mm). This annex requires consideration of risks resulting from disclosure or release.

2. Information Request Requirements. At a minimum, requests to release COMSEC information to foreign governments and international organizations will contain the following information:

a. Identity of US or binational commands that have an interoperability requirement with the foreign nation or international organization. For each requirement, the request will reference the operational plan or concept of operations plan that explains the interoperability requirement.

b. Scope, duration, and urgency of the COMSEC capability required and a statement of how the requirement is currently being met.

c. Source of cryptographic equipment or other COMSEC material needed to fulfill the requirement. Submitting commanders will coordinate with appropriate Service and cryptographic resource managers to determine the specific equipment source and whether needed equipment will be purchased under FMS of cryptographic device services.

d. Provisions providing for engineering, installation, maintenance, and logistic support.

e. Facility adequacy for storing COMSEC material by recipient.

f. Equipment installation and operation plans and how physical requirements will be met.

g. Requirements for instructional material translation, such as operating or maintenance instructions.

h. Requirement milestones and impact if milestones are not met.

C-G-C-1

Annex C  
Appendix G  
Enclosure C**FOR OFFICIAL USE ONLY**

3. Validation. Requests will be forwarded through combatant command channels to the Joint Staff, J-6, for validation prior to submission to the CNSS. See CJCSI 6510.06 (reference mm) for further guidance.

ANNEX D TO APPENDIX G TO ENCLOSURE C

COMSEC MONITORING

1. General

a. The purpose of COMSEC monitoring is to provide unique material, not readily available through other sources, to evaluate the status of US communications (including voice and data transmissions). Information collected through COMSEC monitoring is similar to information available to foreign powers through their SIGINT collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide comprehensive data for analysis. COMSEC monitoring is used to provide the empirical data needed to identify and correct vulnerabilities in accordance with DODD 4640.6 (reference tt) and NTISSD No. 600 (reference uu).

b. USG agencies and departments conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to government telecommunications and to aid in countering telecommunication vulnerability and assist in force protection matters.

(1) US military forces conducting COMSEC monitoring activities must be in strict compliance with applicable statutes, regulations, executive orders, and presidential directives. NTISSD No. 600 (reference uu) provides the national policy on COMSEC monitoring.

(2) Government telecommunications systems are subject to COMSEC monitoring by duly authorized government entities (as specified by individual department or agency regulations). Users of these systems must be properly notified in advance, in accordance with guidelines in this manual, that system usage constitutes implied consent to monitoring for COMSEC purposes.

(3) Military forces will not monitor telecommunications systems owned or leased by government contractors for their own use without first obtaining the express written approval of the contractor's chief executive officer (or designee) and the written opinion of the department or agency general counsel actually performing the monitoring.

(4) Military forces will not monitor, for COMSEC purposes, the contents of telecommunications when such monitoring constitutes electronic surveillance in a law enforcement or investigative sense.

(5) COMSEC monitoring results will not be used to produce foreign intelligence or CI as defined in EO 12333 (reference ww). However, the results of COMSEC monitoring of US and allied military exercise communications may

C-G-D-1

Annex D  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

25 March 2003

be used for intelligence purposes under procedures prescribed in applicable directives.

(6) No department or agency may monitor, for COMSEC purposes, another department or agency's telecommunications without the express prior written approval of the head (or designee) of the department or agency to be monitored, except as provided for in DODD 4640.6 (reference tt).

(7) COMSEC monitoring will be conducted in strict accordance with operational procedures minimizing the possibility that unnecessary communications content will be acquired. Such procedures will be consistent with guidelines approved in writing by the general counsel of the department or agency issuing the procedures.

(8) Technical surveillance countermeasures, electronic sweeps, surveillance of noncommunication emissions (e.g., radar), and TEMPEST testing are not within the scope of COMSEC monitoring.

## 2. Guidelines for the Conduct of COMSEC Monitoring

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 1 above:

(1) To collect operational signals needed to measure security achieved by US codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis for assessing the types and value of information subject to loss through government telecommunications intercept and exploitation.

(3) To provide an empirical basis for improving the security of government telecommunications against SIGINT exploitation.

(4) To help in determining the effectiveness of EA and EP, cover and deception actions, and OPSEC measures.

(5) To identify government telecommunications signals exhibiting unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide adversary SIGINT the capability to identify specific targets for exploitation purposes.

(6) To provide empirical data to train government telecommunications system users in proper IA techniques and measures.

(7) To evaluate the effectiveness of IA education and training programs.

C-G-D-2

Annex D  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

(8) To train personnel and test the capability of COMSEC monitoring equipment.

(9) To determine OPSEC indications that can be obtained from telecommunications to support OPSEC surveys.

b. The following categories of telecommunications are considered public for purposes of this manual. Accordingly, acquisition of any communications in these categories occurring in the course of locating or examining government telecommunications is not electronic surveillance.

(1) Radio or television broadcast communications, whether commercial, public, or educational, intended for public information or entertainment.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the government for public use or access.

(3) Communications in portions of the electromagnetic spectrum that are allocated by the government for its own use.

c. No incidentally acquired nonpublic communication, as defined above, may be monitored beyond the point where a determination can reasonably be made that it is nonpublic. A record of the acquisition may be kept for signal identification and avoidance purposes. Such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the parties or content of the communication.

d. Contents of any nonpublic communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a government communication.

e. Notice of the existence of COMSEC monitoring can be accomplished by any of the following means or any combination thereof, which the affected department or agency legal counsel considers legally sufficient:

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memorandum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the SOPs, communications-electronics operating instructions, or similar documents.

f. In accordance with ASD(C3I) memorandum, "Policy on Department of Defense Electronic Notice and Consent Banner" (reference xx), see Appendix C to Enclosure C, "Electronic Notice and Consent Banner." All DOD information systems must display, as a minimum, an electronic log-on notice and consent banner that advises users of the following principles:

(1) The system is a DOD system.

(2) The system is subject to monitoring.

(3) Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.

(4) Use of the system constitutes consent to monitoring.

### 3. Control of Monitoring Records and Equipment

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring that identify security weaknesses of the monitored activity will be classified at the security level of the system and downgraded to UNCLASSIFIED when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes, except as provided for in paragraph 3e of this annex. These reports will not contain any information extraneous to COMSEC purposes, individual names, or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes will be destroyed as soon as operationally feasible, except in accordance with procedures approved by the attorney general. Information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring and computer-penetration testing activities relating directly to any suspected crime will be referred to the military commander or law enforcement agency having jurisdiction. When taking such action, the general counsel of the department or agency performing the COMSEC monitoring will be notified promptly. COMSEC monitoring results



25 March 2003

may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency performing the monitoring.

d. Information extraneous to COMSEC purposes will not be recorded, reported, noted, logged, or filed, except as provided for in paragraph 3e of this annex. If within the capabilities of COMSEC monitoring equipment, any such information inadvertently acquired will be expunged. All monitoring records will be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes will be limited to that which is necessary for COMSEC purposes. No access to or dissemination of such materials beyond COMSEC operational elements will be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment will be safeguarded to prevent unauthorized access and use.

4. Joint COMSEC Monitoring Support. Monitoring support for COMSEC can be requested from the Joint COMSEC Monitoring Activity (JCMA).

a. The JCMA is a JCS-sponsored, Joint service activity at NSA that provides direct support to the US warfighting joint commands. JCMA's support includes COMSEC monitoring, a search for vulnerabilities with the intent of helping the warfighter improve policies, procedures, and practices, and security architectures. Additionally, operational force protection support, provided mainly during real-world military operations, focuses on the immediate reporting of information exposed in open communications that may jeopardize lives or missions. Monitoring and force protection support are conducted by customer invitation only, and information developed through these means is treated as proprietary to the tasking organization or command.

b. Information on JCMA's support may be obtained from the Customer Support Officers in JCMA/X525, DSN 244-6046 (STU-III capable) or at <http://www.nsa.smil.mil/producer/jcma/>. Requests for support must originate at the "owning" unified command level. JCMA prioritizes each request for support based on the nature of the event and availability of organic and tasked resources; force protection missions receive our given highest priority.

c. Information requests should include the following:

- (1) Units and/or organizations involved or affected.
- (2) Dates and/or times of the event(s) requiring JCMA coverage.

C-G-D-5

Annex D  
Appendix G  
Enclosure C

**FOR OFFICIAL USE ONLY**

- (3) Specific location(s).
- (4) Essential elements of friendly information.
- (5) Technical data related to requested monitoring: frequencies, IP addresses, phone numbers, etc.
- (6) Any background information that would help JCMA.

APPENDIX H TO ENCLOSURE C

PROTECTION MECHANISMS -- LEVELS OF CONCERN AND ROBUSTNESS

1. Levels Of Concern. All DOD information systems will employ protection mechanisms in accordance with the level of concern (i.e., high, medium, or basic) that satisfy corresponding criteria for high, medium, or basic levels of robustness. See Table C-H-1.

a. DOD information systems processing classified information as defined by DOD 5200.1-R (reference i) are assigned a high level of concern. Such systems will employ only NSA-certified, high-robustness IA products when the information transits public networks or the system or network handling the information is accessible by individuals who are not cleared for the classified information on the system.

b. DOD information systems that meet the criteria of national security systems as delineated by 10 USC 2315 (reference yy) and process only sensitive unclassified information are assigned a medium level of concern. Such systems will employ IA products that satisfy the requirements for at least medium robustness when the information transits public networks or the system or network handling the information is accessible by individuals who are not authorized to access the information on the system.

Security Service	Level of Concern/Robustness		
	High	Medium	Basic
Availability		Mission-critical over an unencrypted network.	1. Mission support and administrative over any network. 2. Mission-critical over an encrypted network.
Integrity, Nonrepudiation		1. Mission-critical over an unencrypted network. 2. Network management commands over an unencrypted network.	1. Mission-critical over an encrypted network. 2. Mission support and administrative over any network. 3. Network management commands over an encrypted network.

Table C-H-1. Security Services Robustness

c. DOD information systems processing sensitive information as defined in section 20 of the NIST 15 USC 278g-3 (reference zz) are assigned a basic level of concern. Such systems will employ IA products that satisfy the requirements for at least basic robustness when the information transits public networks or the system or network handling the information is accessible by individuals who are not authorized to access the information on the system.

d. DOD information systems that allow open, uncontrolled access to information through publicly accessible web servers or unregulated access to and from the Internet are also assigned a basic level of concern and will employ mechanisms to ensure availability and protect the information from malicious tampering or destruction. Such systems will also be isolated from all other DOD systems. The isolation may be physical, or may be implemented by technical means such as an approved boundary-protection product.

2. Levels of Robustness. Robustness describes the strength of mechanism (the strength of a cryptographic algorithm) and design assurance (confidence measures taken to ensure proper mechanism implementation) for a technical IA solution.

a. Technical IA solutions in the defense-in-depth strategy will be at one of three defined levels of robustness – high, medium, or basic – corresponding to the level of concern assigned to the system.

(1) Designating levels indicates a degree of robustness of the solution. Evaluation assurance levels (EALs) as defined in the international common criteria (CC), and classes of certificates as defined in the DOD certificate policy, indicate a degree of confidence in the security attributes of the products to which they relate. As security mechanisms improve over the years, the robustness of security products should also improve, and products that are more robust can be incorporated in security solutions. The more robust a particular security attribute, the greater the level of protection it provides to the security services it supports.

(2) Assigning levels of robustness for integrity, availability, and confidentiality for all DOD information systems is another means for ensuring the most cost-effective and best use of IA solutions, including COTS solutions. When implementing IA solutions, they will be at a designated robustness level commensurate with the level of concern, except where noted. It is also possible to use nontechnical measures to achieve protection requirements dictated by the level of concern. For example, physical isolation and protection of a network can be used to provide confidentiality. In these cases, the technical solution requirement may be reduced or eliminated.

(3) The three levels of robustness discussed below are based on the robustness strategy presented in the IATF. It should be noted that today's technology could support development of protection that is more stringent and with rigorous security countermeasures; however, development costs would far exceed acceptable budget limits. Therefore, the term "high robustness" used here is relative to the other levels of robustness, including those of the IATF robustness strategy, and does not indicate the best that could be developed in a fiscally unconstrained environment. The three levels of technical robustness solutions are described below.

b. High-robustness security services and mechanisms provide the most stringent protection and rigorous security countermeasures. High-robustness solutions require all of the following:

(1) NSA-certified type 1 cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash.

(2) NSA type 1 cryptographically authenticated access control (e.g., digital signature, public key cryptography-based, challenge and/or response identification and authentication).

(3) Key management, requiring:

(a) For symmetric key, NSA-approved key management (production, control, and distribution).

(b) In the future, for asymmetric key, class 5 public PKI certificates and hardware security tokens that protect the user's private key and crypto-algorithm implementation.

(4) High-assurance security design, such as specified by NSA or the international CC, at a minimum, an EAL greater than 4.

(5) Products evaluated and certified by NSA.

c. Medium-robustness security services and mechanisms provide for additional safeguards above the DOD minimum. Medium-robustness solutions require, at a minimum, all of the following:

(1) NIST FIPS 140-2 level 2 (reference aaa) validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table C-10) as specified in NSTISSAM INFOSEC/1-00 (reference pp).

(2) NIST cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge and/or response identification and authentication).

(3) Key management, requiring:

(a) For symmetric key, NSA-approved key management (production, control, and distribution).

(b) For asymmetric key, class 3 PKI certificates and hardware security tokens that protect the user's private key.

(4) Good assurance security design such as specified in CC as EAL 3 or greater.

(5) Solutions evaluated and validated under the common criteria evaluation validation scheme or NSA.

(6) Solutions for national security systems approved by NSA.

d. Basic-robustness solutions are equivalent to good commercial practice. Basic robustness requires, at a minimum, all of the following:

(1) NIST FIPS 140-2 level 1 or 2 (reference zz) validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table C-H-4) as specified in NSTISSAM INFOSEC/1-00 (reference pp).

(2) Authenticated access control (e.g., digital signature, public key cryptography-based, challenge and/or response identification and authentication, or pre-placed keying material).

(3) Key management, requiring:

(a) For symmetric key, NIST-approved key management (production, control, and distribution).

(b) For asymmetric key, class 3 PKI certificates or pre-placed keying material.

(4) CC EAL 1 or greater assurance.

(5) Solutions evaluated and validated under the NIAP common criteria evaluation validation scheme or NSA.

e. While paragraph 2 focuses on the robustness of individual security services and mechanisms, the robustness of a network solution must be considered in the context of defense-in-depth and the threat environment in which the system operates. For instance, a system operating on a protected backbone between secure enclaves may not require additional mechanisms for authentication and access control. In addition, if community of interest separation is provided through encryption, it will require less robust solutions.

f. The tables below are tools for use in a disciplined system security engineering approach for building or replacing systems. They cover the major defense-in-depth areas but are not all-inclusive for every system requirement and should not be used as a substitute for good systems security engineering. The robustness indicated is the minimum that should be considered for the defense-in-depth application in the environment listed. However, solutions that are more robust should always be considered during the in-depth security analysis of system requirements. In addition, as IA technology improves and systems are replaced or upgraded, higher-robustness solutions should always be considered.

3. Security Services Robustness. Availability ensures that the resources and data are in place, at the time and in the form needed by the user. Availability is enhanced by access control, which limits access to authorized users only. Integrity ensures that data has not been altered or destroyed and is achieved using digital signatures or keyed hash schemes. Nonrepudiation provides the ability to prove to a third party that an entity did indeed participate in a communication. Nonrepudiation is provided by the authenticating characteristics of digital signatures. Minimum-robustness requirements for availability, integrity, and nonrepudiation are shown in Table C-H-1.

4. Access Control Robustness. Access control is used to limit access to networked resources (hardware and software) and data (stored and communicated). The main elements of access control are identification and authentication and authorization. Passwords, tokens, and certificates are used to achieve authenticated access control at the workstation and host level. Table C-H-2 gives examples of minimum-robustness requirements for access control mechanisms in particular situations.

Defense-in-Depth Application examples	Level of Concern/Robustness for Access Control	
Defending the Network	Encrypted and/or physically isolated network	Unencrypted or not physically isolated network
Access to DOD network management centers and all network management control commands to managed GIG components (e.g., routers, switches), as well as inter-element commands (e.g., router table propagation)	Basic	Medium
Defending the Enclave	Encrypted and/or physically isolated network	Unencrypted or not physically isolated network
All interconnections between enclaves or LANs operating at different classification levels, (e.g., TOP SECRET to SECRET, SECRET to UNCLASSIFIED) or between US and foreign nation systems or networks will only be through a NSA approved well-defined and controlled gateway.	Medium + (The level of robustness for this case, which is also known as a high assurance guard, is medium; however, additional design assurance is required and must have an EAL greater than 4.)	Medium + (The level of robustness for this case, which is also known as a high assurance guard, is medium; however, additional design assurance is required and must have an EAL greater than 4.)

Table C-H-2. Access Control Robustness Examples



Defending the Enclave	Encrypted and/or physically isolated network	Unencrypted or not physically isolated network
(NOTE: Connection between different classification levels allow lower classified or unclassified data from the higher classified system to be moved to the lower classified or unclassified system (e.g., unclassified data on a SECRET system to an unclassified system). In addition, unclassified data from an unclassified system can be moved to a classified system with the use of a well-defined and controlled gateway.		
All boundaries between Enclaves at the same sensitivity level and the WAN will be protected. (NOTE: All gateways at boundaries between enclaves and WAN will contain an intrusion detection and attack sensing and warning capability. All interconnections between enclaves or LANs operating at different classification levels should be designed and analyzed to reduce covert channels.)	Basic	Basic for mission support and administrative information. Medium for mission-critical.
Defend the Computing Environment	Encrypted and/or physically isolated network	Unencrypted or not physically isolated network
User log-on to a workstation to gain access to network resources	Basic	Basic

Table C-H-2. Access Control Robustness Examples (cont'd)

Defend the Computing Environment	Encrypted and/or Physically Isolated Network	Unencrypted or not Physically isolated Network
User access to servers (e.g., Web servers, database servers, file servers) or other components storing special compartmented, special access, or other mission-critical information, will use authenticated access.	Basic	Medium
User accesses to servers (e.g., Web servers, database servers, file servers) or other components storing mission support or administrative, will use authenticated access.	Basic	Basic
All Network Management control commands to managed GIG components (e.g., routers, switches), as well as inter-element commands (e.g., router table propagation) in the Enclave will employ authentication.	Basic	Medium
All mission-critical, mission support and administrative transactions, to include individual (non-organizational) E-mail and E-commerce, will be secured with a digital signature.	Basic	Basic- for mission support and administrative information medium- for mission-critical information

Table C-H-2. Access Control Robustness Examples (cont'd)

## 5. Encryption

a. Encryption is a procedure to convert plain text into cipher text. Within the Department of Defense it is used for:

(1) Confidentiality. To ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes.

(2) Data Separation. To ensure that information of different classifications sharing the same transport (transmission) media are not commingled.

(3) Privacy. To ensure that information at the same classification level is kept separate based on need to know.

b. Table C-H-3 provides robustness guidance for data encryption robustness. Note that when information is encrypted for the purposes of data separation or privacy, it is always tunneled through a network that is also encrypted for confidentiality.

Purpose of Encryption	Data classification/Network Type	Minimum Robustness of Algorithm
Confidentiality	TOP SECRET through SECRET	High
	TOP SECRET through Commercial	High
	SECRET through Commercial	High
	SECRET through SECRET Releasable to Allies/Coalition	High
	UNCLASSIFIED SENSITIVE through Commercial	Basic
Data Separation	SECRET through TOP SECRET	Medium
	UNCLASSIFIED through TOP SECRET	Medium
	SECRET Releasable to Allies/Coalition through SECRET	Medium
	UNCLASSIFIED through SECRET	Medium
Privacy	TOP SECRET through TOP SECRET	Basic
	SECRET through SECRET	Basic
	UNCLASSIFIED through UNCLASSIFIED SENSITIVE	Basic

Table C-H-3. Data Encryption Robustness

6. Cryptographic Functions. Cryptographic functions include encryption, hash, signature, and key exchange algorithms. These algorithms are used to

protect the confidentiality and/or integrity of information. Table C-H-4 lists currently available algorithms. It includes algorithms that are often encountered in commercial products primarily for reference purposes. The number of bits or the length of the cryptographic key used in the algorithm and the design assurance of the algorithm are directly related to its robustness and will determine whether the NIST-certified algorithms listed in Table C-H-2 are basic or medium robustness. Within the Department of Defense, only NSA- or NIST-certified cryptographic algorithms may be used unless otherwise authorized. See Chapter 4 of the IATF (<http://www.iatf.net>) for a detailed description of algorithm robustness.

Algorithm	Commercially Available	NIST-Certified Basic/Medium Robustness	NSA-Certified High Robustness
Encryption Algorithm	RC4 RC5 IDEA Blowfish	AEA DES SKIPJACK	Contact NSA
Hash Algorithm	MD5 New standards as available	SHA 1 New standards as available	Contact NSA
Signature Algorithm	RSA EDSA	DSA	Contact NSA
Key Exchange Algorithm	RSA DH	KEA	Contact NSA
AEA- Advanced Encryption Algorithm DES- Digital Encryption Standard DH- Diffie-Hellman DSA- Digital Signature Algorithm EDSA- Elliptic Digital Signature Algorithm Hash- One way mathematical operation		IDEA- International Data Encryption Algorithm KEA- Key Exchange Algorithm MD5- Message Digest 5 RSA- Rivest-Shamir-Adleman SHA- Secure Hash Algorithm	

Table C-H-4. Algorithm Robustness Examples

## APPENDIX I TO ENCLOSURE C

## INTERCONNECTION AND DATA TRANSFER BETWEEN SECURITY DOMAINS

1. Description. This appendix:

- a. Provides DOD procedures, in accordance with DODD 8500.1 (reference bbb), DODI 5200.40 (reference f), DOD 8510.1-M (reference ccc), and DITSCAP Implementation manual (reference ccc), for the interconnection of information systems of different security domains and the engineering, installation, certification, accreditation, and maintenance of such interconnections.
- b. Implements the requirements of the IC CIO TSABI (reference ddd) within the Department of Defense for connecting TOP SECRET/SCI information systems with systems of lesser classification.
- c. Prescribes procedures for dissemination or transfer of data across security domains.
- d. Defines the characteristics of the required controlled interface (an element of which is commonly referred to as a "guard") between security domains and implements the requirements of Director of Central Intelligence Directive (DCID) 6/3 (reference eee) within the Department of Defense for controlled interfaces connecting intelligence systems with systems of lesser classification.

2. Background

- a. Interconnection of information systems of different security domains may be necessary to meet essential mission requirements. The operational need for each interconnection must be balanced with the risk associated with the interconnection to the confidentiality, integrity, and availability of the affected information systems. Such connections pose significant security concerns (including possible disclosure of classified information to unclassified users, thus compromising the integrity of classified systems) and will be employed only to meet compelling operational requirements, not operational convenience. Application of security configurations with approved security products, uniform risk criteria, trained systems security personnel, and strict configuration control is necessary to mitigate risk. If the interconnection affects more than one DAA, the lead DAA will ensure that the community risk is assessed and measures taken to mitigate that risk must be adopted prior to interconnecting the systems.

25 March 2003

b. DAAs must validate the operational requirement for all connections between security domains prior to developing engineering solutions. All such connections must be designed, developed, integrated, certified, and accredited as part of the DITSCAP and documented in an SSAA in accordance with DODI 5200.40 (reference f) and DOD 8510.1-M (reference ccc). Special procedures within the DITSCAP, including registration with the DISN SCAO, review as part of the GIAP and community-wide risk assessment by the DSAWG, must be followed as described in paragraph 2d and Annex A of this appendix, "Interdomain Data Transfer: Generic Framework and Scenario."

c. Transfer of data across security domains requires data attribution and data review prior to release and must be supported by automated tools on a trusted host with an appropriate level of robustness. This process is described in paragraph 3 and defined by a generic framework (see Annex A of this appendix, "Interdomain Data Transfer: Generic Framework and Scenario"). Consistent security policy and procedures for transfers are essential so that acceptable implementations are fielded within the Department of Defense.

d. Interdomain connections will be reviewed semi-annually to ensure that a valid operational requirement for the connection still exists and the current implementation satisfies the requirement. Because these connections are high risk, they will be recertified and reaccredited annually. Recertification will include an independent vulnerability assessment of the connection.

e. Only guarding solutions accredited by the DISN DAAs or the IC Principal Accrediting Authorities may be used to interconnect information systems of different security domains.

### 3. DITSCAP Procedure for Interconnection of Security Domains

a. General. Procedures within the DITSCAP described in DODI 5200.40 (reference f) and DOD 8510.1-M (reference ccc) must be followed in acquiring, operating, and maintaining connections between information systems connecting security domains. These procedures will be developed and maintained by the NSA Guarding Solutions Office (GSO) for collateral interconnections and by the NSA TSABI Program Office for TOP SECRET/SCI and below interconnections. The collateral inter-domain interconnection process is described in the following paragraphs and in Annex A and conforms to the four phases described in the DITSCAP. While the TSABI process is very similar, DOD components must follow the IC CIO TSABI policy (reference ddd) for TOP SECRET/SCI connection procedures.

#### b. DITSCAP Phase I (Definition) - Initiation

(1) As part of the functional requirement development, the program manager develops the requirements and system descriptions and other DITSCAP data needed to begin the DITSCAP.

(2) After assembling the necessary data, the program manager contacts the DAA, who must validate the operational requirement for the inter-domain connection prior to the development of engineering solutions. The DAA, in coordination with the SCAO (as required) determines whether the requirement requires the connection of systems across security domain boundaries and entry into the GIAP.

(3) Upon determining that the requirement is within the scope of GIAP, the DAA completes the DITSCAP registration task requirements (including mission, function, system descriptions, and a draft SSAA) and registers with the SCAO, entering the required information into the GIAP registration database.

(4) Based on the information provided by the program manager, the DAA and GSO (as required) determine if a referenced implementation (RI) exists.

(a) If an RI exists, the program manager and DAA estimate the level of effort required to implement the RI, such as design documentation, development, and testing along with schedule, staffing levels, and cost information. Upon review and approval by the DAA, the information is entered into the GIAP database for tracking purposes.

(b) If an RI does not exist, the program manager and DAA define the architecture for a new controlled interface. In defining the architecture, the program manager and DAA, in consultation with the GSO, must ensure the new controlled interface satisfies all of the controlled interface requirements (see Annex B of this appendix, "Controlled Interface Characteristics"). They must also consider any specific community risk issues that the solution must address.

(5) The program manager and DAA assess whether the new controlled interface fully satisfies their overall requirements. If the interface can only partly satisfy the requirements, the program manager and DAA may have to readdress or change the functional and operational requirements of the information system or the architecture for the controlled interface. This will temporarily end the process, which can be restarted with a redefined requirement or architecture. If the controlled interface fully satisfies their overall requirements, they can proceed to the DITSCAP verification phase.

c. DITSCAP Phase II (Verification) – Development and Acquisition

(1) The program manager and DAA review and approve the design and development schedule and update information in the GIAP database.

(2) The program manager and DAA, with GSO support as necessary, plan the system security engineering survey (SSES) activities. If the SSES expertise is available locally, the program manager and DAA select the organization to provide the support. If the expertise is not locally available, the GSO will assist in identifying potential SSES support. The information will be entered into the GIAP database.

(3) With SSES team support, the program manager and DAA design, develop, integrate, and test the controlled interface in the laboratory and at the site. The SSES team will usually identify and evaluate potential solutions by analyzing an existing solution (such as an RI) and customize it for the site. The extent of this phase is dependent on whether the proposed solution has been implemented elsewhere and is documented as an RI. This information, which is essential to the following certification, risk assessment, and GIAP reviews, must be documented in a site survey report and included in the SSAA.

(a) Controlled interface solutions, especially those not based on an RI and requiring a community risk assessment, must be coordinated with the affected community during this phase.

(b) Community involvement depends upon the information system connectivity. For all systems connected to the DISN, the DSAWG represents the DISN DAAs and DISN “community.” The DSAWG will also provide the DOD community risk assessment for DOD collateral systems not connected to the DISN, but which are being connected across security domains. For TOP SECRET/SCI systems, the Defense and Intelligence Community Accreditation Support Team (DICAST) represents the DOD/IC TOP SECRET/SCI community.

(c) Community guidance should be carefully considered in developing the controlled interface solution, since ultimately the approval to operate the connection will be a community decision.

d. DITSCAP Phase III (Validation) – Implementation - Local and Community Risk Assessment

(1) During the validation phase, the DAA with program manager and SSES team support as required, must determine if the risk associated with this implementation is local or affects a larger community.



(a) Local risk is assessed and accepted or rejected by the DAA.

(b) Community risk requires community acceptance. An MOA is required between DAAs of the connected systems. The MOA should name a lead DAA responsible for the system certification. If no lead DAA is named, the system will be jointly certified. Acceptance of risk by all affected DAAs is required. For DOD collateral systems, the DSAWG will provide community risk assessment for DAA consideration. For TOP SECRET/SCI systems, the DSAWG will coordinate with the DICAST.

(2) If the risk is truly local, the DAA performs a local risk assessment and decides whether to accept the local level of risk. If local risk is unacceptable, the PM and DAA may have to readdress or change the functional and operational requirements of the information system or the architecture for the controlled interface. This will temporarily end the process, which can be restarted with a redefined requirement or architecture.

(3) If local risk is acceptable, the community risk must be assessed.

(a) If the DAA considers the community risk unacceptable, the PM and DAA may have to readdress or change the functional and operational requirements of the information system or the architecture for the controlled interface. This will temporarily end the process, which can be restarted with a redefined requirement or architecture.

(b) If the DAA considers the community risk adequately mitigated, the risk analysis must be documented in the SSAA. Upon satisfactory completion of certification testing, the DAA submits a request to operate (RTO) to the SCAO as part of the GIAP process. The SSAA survey report is forwarded to the NSA GSO and DSAWG for review.

(4) The GSO will examine the SSAA survey report from the DAA to insure the technical evidence supports the conclusions and identifies technical errors or missing information. The GSO will also review the risk assessment.

(a) If the DAA identifies the connection as community risk, the GSO will examine and validate the risk assessment and provide any recommendations to the DAA and DSAWG. The DAA must address these recommendations during its review with the DSAWG.

(b) If the DAA assesses the risk as local, the SCAO, GSO, and DSAWG will examine the interconnection requirements and verify that the connection does not have an associated community risk (e.g., DISN). Should the DSAWG determine that there is a community risk, the DSAWG will identify

25 March 2003

the community concerned to the DAA with recommendations for risk mitigation. The DAA will implement the recommendations or withdraw the RTO until the issue is resolved with the affected community.

(5) After addressing the DSAWG recommendations, the DAA finalizes the SSAA. If a community risk, the actions taken to mitigate the risk must be documented as part of the SSAA. This requires a review of the SSAA by the DSAWG and the DISN DAAs.

(a) Community acceptance of the risk is documented by the DAAs in the MOA and SSAA. The final SSAA will be provided to the SCAO.

(b) If the community rejects the risk, the DAA, with support of the program manager and SSES team, will document the problem and identify potential solutions and risk mitigation alternatives. If the solutions are feasible and acceptable to the DAA, the updated SSAA is provided for DSAWG review. If the system problems cannot be solved or if the program manager or DAA choose not to continue the process, the implementation is terminated. If the DAA determines that an overriding operation requirement exists for the connection, the DAA may appeal the community decision to the DOD CIO (or the Director of Central Intelligence for TOP SECRET/SCI systems).

(6) If the solution is not currently an RI, the GSO will examine the suitability of the solution as an RI and, as appropriate, add it to the RI database.

e. DITSCAP Phase IV (Post Accreditation) – Operation and Maintenance

(1) To insure an acceptable level of risk is maintained, DAAs must impose positive configuration control over all inter-domain connections. Changes in configuration will be incorporated in the SSAA and a copy provided to the SCAO. DAAs will review the requirement and operational procedures for all inter-domain interconnections on a semi-annual basis to ensure a valid operational requirement still exists, and the current implementation satisfies the requirement.

(2) DAAs will require complete recertification and reaccreditation, to include penetration testing, vulnerability, and risk assessment, of each inter-domain connection annually. The SSAA will be modified to reflect this certification and a copy provided to the SCAO.

#### 4. Procedure for Data Transfer Across Security Domains

a. This procedure establishes a common framework (see Annex A of this appendix, "Interdomain Data Transfer: Generic Framework and Scenario") for transfers across security domains. In particular, the framework defines a process involving data attribution and reliable human review and release for transferring data across security domains. The objectives of the framework are to promote secure and more controlled manual transfers, interoperable mechanisms and tools for automated transfers, and deployment of a limited and manageable set of transfer solutions.

b. Mechanisms and procedures that support the transfer of data across security domains will conform to the requirements identified in DODD 8500.1 (reference bbb), DCID 6/3 (reference eee), and this appendix.

c. Data targeted for transfer across security domains will be developed, assembled, and structured for ease of review, attribution, and transfer. The data will include the appropriate security markings described in DOD 5200.1-R (reference i). Alternately, for data not intended for human viewing the data classification will be described in the associated system documentation.

d. Data that is transferred to a security domain will possess at least one strong binding (digital signature) with at least a medium level of robustness provided by a designated reliable human reviewer.

e. The producers (e.g., authors or individuals developing or assembling the data being transferred) may employ a strong binding to link or identify themselves with the data they created. The strong binding (e.g., digital signature) will provide proof of origin; namely, the binding will identify the producers that developed (assembled) the data (attribution). The strong binding will also assist with the detection of modification (tampering) of the data.

f. A reliable human review will be performed on data prior to dissemination to the destination security domain. A reliable human reviewer will validate any available producer-to-data binding(s). The validation will ensure that the data has not been tampered with and that the producers associated with the data have been identified. In addition to validating strong bindings, the reliable human reviewer will be responsible (held accountable) for reviewing the content of the data to ensure that no inappropriate information will be disclosed in the destination security domain.

(1) The reliable human reviewer will be provided with automated tools to facilitate the review. The tools will be developed to support the specific information and formats employed to disseminate the data being reviewed.

(2) The automated tools will enforce the review process (the reviewer will not be permitted to disregard elements of the review) and provide evidence that the review has been completed.

(3) The automated tools and the system (workstation) used by the human reviewer must be a trusted platform, certified for a level of trust commensurate with the risks associated with the transfer being conducted.

g. After completing the final review, the reliable human reviewer will provide a strong binding with the approved data and reviewer. The data may then be forwarded for manual transfer, or to an intermediate system or a transfer device (guard) for automated transfer.

h. The manual transfer process or guard will validate the data binding(s) to ensure that the data has not been tampered with prior to reaching the transfer point. The manual transfer process or guard may also provide additional functionality such as scanning for malicious code or performing "dirty word" checking. The manual transfer process or guard will cause the security label (the network label) to be altered to represent the destination security domain.

i. After successful validation of data binding(s) by the manual transfer process or guard, the data will be transferred to the destination security domain.

j. The manual transfer process or guard will log (audit) all data-release activities, to include identity of reliable human reviewer, identity of data released, successful or unsuccessful binding validations, and date and time of transfer (release).

k. In the case of data that consists solely of "highly structured/formatted, 7-bit, ASCII text," an accredited, rule-based, text review engine, at the discretion of the DAA, can provide reviewer, releaser, and control interface and transfer functions for data that is highly structured and/or formatted.

1. The DOD CIO will review proposed exceptions or waivers to these procedures.

25 March 2003

## ANNEX A TO APPENDIX I TO ENCLOSURE C

## INTERDOMAIN DATA TRANSFER -- GENERIC FRAMEWORK AND SCENARIO

1. Generic Framework -- Transfer of Data between Security Domains

a. The generic framework for interdomain transfer is shown in Figure C-I-A-1. The entire process is divided into three broad steps: production, review and/or release, and transfer. Although each step is often performed under the control of a particular DOD or IC organization and is restricted to its infrastructure, the steps are separable and, in theory, each could be performed anywhere in the originating domain (backbone network or DOD organization).

b. The data transferred will probably be assembled from a variety of IT assets located anywhere in the originating domain.

(1) The producers creating the data (sources and/or authors) may apply a strong binding, such as a digital signature, to their individual pieces of the assembled data so that the publisher has some assurance about the integrity and origin of each portion. The strong binding provides attribution to an individual person.

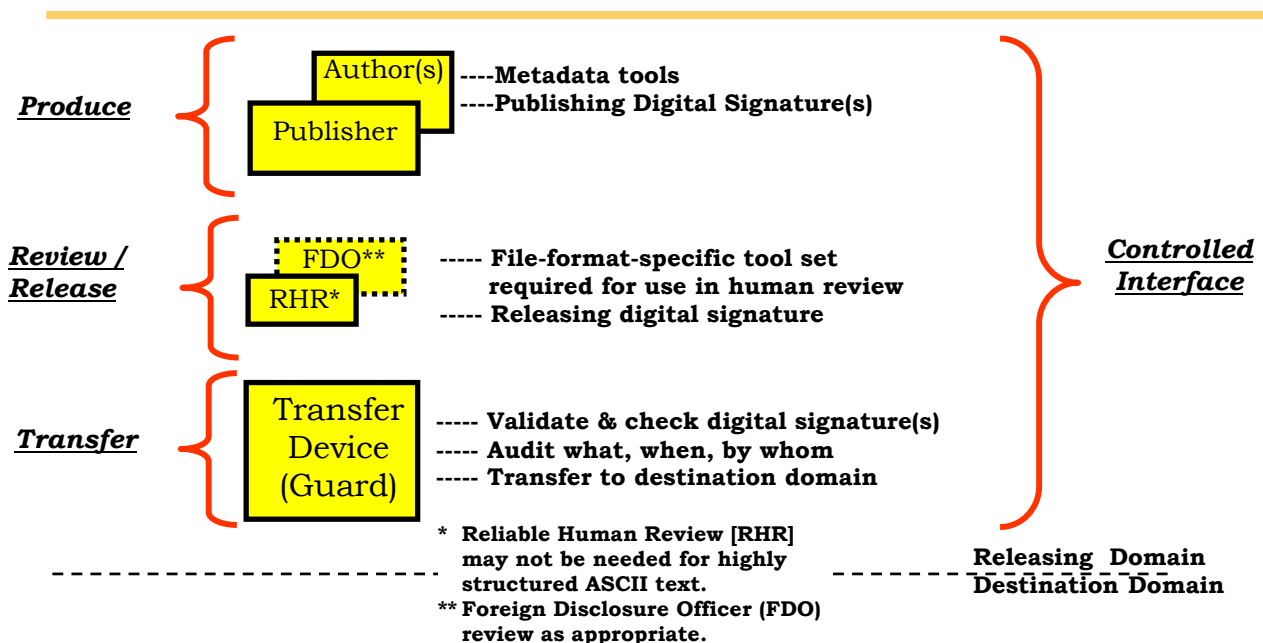


Figure C-I-A-1. Generic Framework for Inter-Domain Transfer

C-I-A-1

Annex A  
Appendix I  
Enclosure C

**FOR OFFICIAL USE ONLY**

(2) The publisher, having assembled and possibly modified the original individual products will, with the proper tool set, ensure that the data (linked composite of individual products) is appropriately scanned, has appropriate security markings, and contains a strong publisher-to-data binding. The publisher applies the strong binding to the compiled (composite) data. The data is now ready for dissemination within its original security domain.

(3) Before the data can be disseminated (transferred) to another security domain, the data must be reviewed and approved for release. A reliable human review (RHR) by a qualified individual other than the producer is required to ensure that the document's contents have not changed (an integrity check), that it contains appropriate security markings, and that its contents are appropriate for those markings.

(a) If the RHR has automated support, file format specific tools are required to aid the review. A FDO might additionally be required to verify that the data is appropriate for dissemination to a foreign nation. If the process is automated in whole or in part, an appropriate suite of tools (specific to the file formats involved) to scan the components (files) of the product will be required to allow for valid review and release.

(b) Data not approved for release (maybe due to a variety of reasons) will be resolved or forwarded back to the producer for resolution. The reviewer or FDO will then apply a strong, reliable, human-reviewer-to-data binding and forward the data to a manual transfer process, an appropriate server for staging, or to a transfer device (guard) for immediate transfer.

(4) The manual transfer process or guard validates the data binding(s) to ensure that the data has not been modified and originated with an authorized RHR (release authority). Only if both conditions are met will the manual transfer process or guard alter, if necessary, the security labels on the data and perform the transfer to the destination security domain. The security label on the data reflects the sensitivity of the originating domain of the product. This label is not embedded in the product but rather is associated with the product (a network label). The appropriate security markings of the data may or may not match the security label at any given point and may not be altered. Whether the data is formally released or rejected by the manual transfer process or guard, the processes will generate an audit record of all relevant information.

(5) A key concept with this framework is that the RHR and transfer processes are separate and distinct. An RHR must be performed on the data

prior to transfer (release) across security domains. An approved manual procedure or guard provides the actual transfer of the reviewed data.

(6) When the data transfer is from a less-sensitive domain to a more-sensitive domain, the actual transfer must occur as a *one-way* process. When the data is received at the more-sensitive domain, the review process and authorized-releaser-check of the product binding are repeated.

(7) As previously noted in subparagraph 4k of this appendix, a highly structured and/or formatted, 7-bit, ASCII text can be processed by a rule-based text engine that also provides both reviewer and/or releaser and controlled interface and/or transfer functions. However, most web-based products are composed of elements that vary greatly in structure, format, and content. Tool suites that automatically scan each component type to insure appropriate integrity, attribution, content, and marking are required for both a reliable review and to speed the transfer process. The practice of allowing non-text files or non-textual components to transfer between security domains without effective human review (aided by tool suites specifically designed for the type of information being transferred) imposes a substantial increase in the residual risk associated with interdomain transfers and is not permitted.

## 2. Interdomain Transfer Scenario

a. Figure C-I-A-2 shows an example scenario of an inter-domain transfer process. The scenario involves the creation, RHR, and transfer of a web-based product (document).

b. This scenario expands on the generic transfer process described in the main body of this appendix, providing a graphic depiction of automated transfer and product signing. The scenario makes use of a PKI (DOD/IC PKI) where individual users are issued X.509v3 (or most current approved) digital certificates for use with PKI-enabled applications. PKI-enabled applications can apply and validate digital signatures with objects (e.g., E-mail, forms, and documents). For example, a document-signing tool that incorporates digital certificates may be employed to digitally sign a document. The tool can also be used to validate the digital signature to ensure that the document has not been modified.

c. The process starts with author creation of a product or product element (includes metadata), which is then signed using the author's digital certificate. The digital signature establishes the origin of the product or product element (attribution). The author then pushes the signed product or product element to the publisher processes, which may reside on a finished product server.

C-I-A-3

Annex A  
Appendix I  
Enclosure C

**FOR OFFICIAL USE ONLY**

d. The publisher processes are used for establishing the identity of the product or product element and its author(s) by validating the author(s) digital signature, as well as providing product assembly if the final product is composed of multiple product elements. (If various authors provide product elements, the publisher may be responsible for product assembly.) The metadata is checked and updated if necessary by the managing publisher. The managing publisher, after reviewing the final product, signs the product. The product is then forwarded to the release authority (RA) processes, which may reside on a releasable product server.

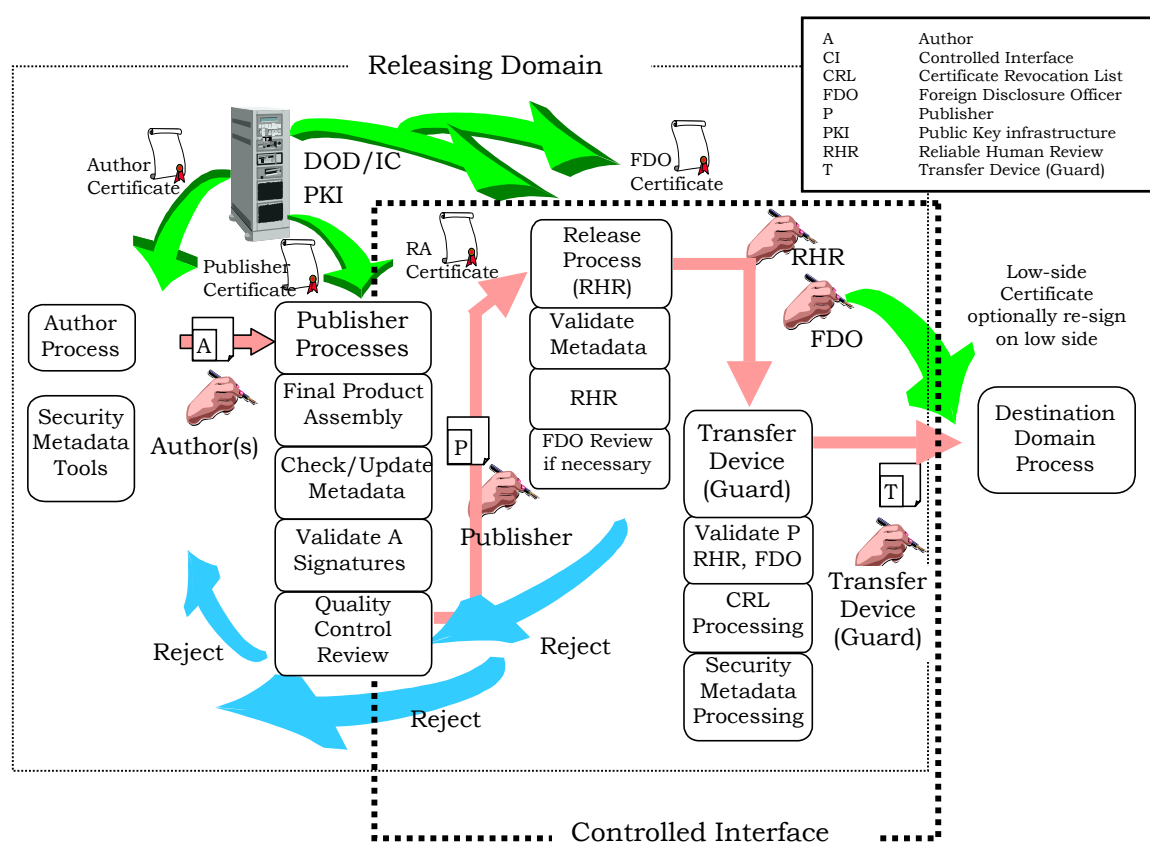


Figure C-I-A-2. Example Automated Transfer Process Scenario

e. The RA processes are used to validate the publisher's digital signature and the metadata associated with the product. The RA processes are also used to provide the final human review and releasability checks. The product is reviewed by appropriate RA and possibly an FDO. (Note that the RA and FDO could be the same person, depending on the CONOPS.) These reviews may



include “dirty word” searches and virus scans. The RA and FDO signatures, if appropriate, are added to the releasable product. The product is then sent to a transfer device (guard). The guard performs the final check on the digital signatures and the metadata to check for releasability. The product will not be released by the guard if the release signature is not that of an approved releaser. The guard logs (audits) the transaction. Certificate revocation list processing may also be performed at the guard.

(INTENTIONALLY BLANK)

C-I-A-6

Annex A  
Appendix I  
Enclosure C

**FOR OFFICIAL USE ONLY**

## ANNEX B TO APPENDIX I TO ENCLOSURE C

## CONTROLLED INTERFACE CHARACTERISTICS

1. Controlled Interface Overview

a. A controlled interface (e.g., guard or firewall) is a mechanism that facilitates adjudicating the security policies of different interconnected information systems (controlling the flow of information into or out of an interconnected information system). Controlling the flow of information into an interconnected information system helps preserve the integrity of the system and the integrity and confidentiality of the information maintained and processed by the system. Controlling the flow of information out of the system helps preserve the confidentiality of the information leaving the system and may protect the integrity of the receiving information systems. The adjudication of integrity and confidentiality policies may be handled in variety of ways. For example:

(1) A single controlled interface may perform all of the confidentiality and integrity adjudication.

(2) One controlled interface may be employed for adjudicating confidentiality policies while another adjudicates integrity policies.

(3) The adjudication of confidentiality and integrity policies may be distributed across a set of controlled interfaces where each performs some subset of confidentiality and integrity policy adjudication. In this instance, the set of controlled interfaces adjudicates all of the required integrity and confidentiality policies.

b. While a controlled interface is often implemented as a mechanism (or a set of mechanisms) separate from the information systems it is intended to protect, this need not be the case. A controlled interface can be constructed so that some of its functionality resides in the information systems themselves. Regardless of its implementation, the controlled interface must conform to the requirements of DODI 8500.2 (reference w).

2. Common Controlled Interface Requirements

a. Each controlled interface must be configured and located to facilitate its ability to provide controlled communication between the interconnected systems.

b. The requirements imposed upon controlled interfaces do not release the DAA, IAO, or IAM of the obligation to ensure that the information systems comprising the interconnected information system provide the required security functionality.

c. The introduction of a controlled interface does not impact the determination of the MAC or the confidentiality level of the information systems comprising the interconnected information system.

d. The availability level of concern of each controlled interface will be at least as high as the lowest availability level of concern of the interconnected information systems as established by DODI 8500.2 (reference w).

### 3. Controlled Interface Confidentiality Requirements

a. A controlled interface will be required for facilitating the adjudication of confidentiality policies if the two interconnected information systems are approved to process information of different classifications.

b. A controlled interface will be required for facilitating the adjudication of confidentiality policies if the compartments, sub-compartments, caveats, control markings, or special handling of information processed by one interconnected information system is different than the compartments, sub-compartments, caveats, control markings, or special handling of information processed by the other interconnected information system.

c. The security requirements imposed upon confidentiality controlled interfaces are based on their constrained operation and function so that information that flows through the controlled interface is generally push-only or pull-only. In those instances where the controlled interface supports both push and pull capabilities, some other constraint limits the bandwidth or format of information flowing through (e.g., information may be limited to a fixed format or users may be limited to a set of fixed-format queries). More stringent requirements must be applied where information is flowing between systems approved to process different security levels or compartments, such as those in use by the IC, and the information flow is not constrained in some manner similar to that described above. For interconnections of TOP SECRET/SCI to collateral or unclassified domains, the controlled interface must comply with DCID 6/3 (reference eee) and meet its Protection Level 4 (to TOP SECRET/SCI) or Protection Level 5 requirements (for connection to unclassified).

#### 4. Controlled Interface Integrity Requirements

a. A controlled interface facilitating the adjudication of integrity policies will control all information flows into an interconnected information system.

b. The integrity requirements of controlled interfaces are determined through the SSES process, and are impacted by circumstances such as an information system sending information to the controlled interface, which in turn is directly connected to another system accessible by users holding a lower clearance. At a minimum, the controlled interface complies with the baseline integrity controls identified through DODI 8500.2 (reference w).

c. Providing integrity features in the controlled interfaces does not relieve the interconnecting systems of responsibility for providing the same features. For example, even though the control interface reviews incoming information for malicious code, the receiving information still has a responsibility to check incoming information (including that from the controlled interface) for malicious code.

(INTENTIONALLY BLANK)

C-I-B-4

Annex B  
Appendix I  
Enclosure C

**FOR OFFICIAL USE ONLY**

## APPENDIX J TO ENCLOSURE C

## MOBILE CODE

1. Purpose. This appendix provides guidance to implement CJCSI 6510.01 (reference b) on use of mobile code in DOD information systems.

2. Background

a. CJCSI 6510.01 (reference b) establishes joint DOD-wide policy on the use of mobile code in DOD information systems and computers. The mobile code and mobile code technologies are defined below:

(1) Mobile code is software obtained from remote systems and downloaded and executed on a local system (e.g., a computer with a web browser) without explicit installation or execution by the recipient.

(2) Mobile code technologies are software-based technologies that facilitate the production and use of mobile code (e.g., Java, JavaScript, VBScript, and ActiveX).

(3) DOD mobile code policy applies to mobile code obtained from sources outside the user's own enclave.

(4) DOD mobile code policy does not apply to use of mobile code downloaded from within the confines of the user's enclave.

b. There are three primary risk categories for mobile code. Each risk category has specified usage restrictions and development and procurement restrictions for mobile code technologies assigned to it. Specific mobile code technologies undergo a risk assessment and are assigned to one of the three primary risk categories. Additional mobile code technologies will be assigned to specific risk categories after risk and/or benefit assessments are completed. The fourth category, the emerging technology category, includes technologies that have not yet been categorized. The assignment of mobile code technologies to risk categories will be reviewed at least quarterly, enabling an updated technology to be reassigned to a different risk category in a timely manner if its risk assessment changes. The categories and the associated restrictions are summarized below.

3. Definitions. This appendix uses specific definitions for some of its terms. Because some of these definitions are unique or differ from common usage,

understanding these terms is critical to understanding the scope and requirements of DOD policy and this appendix.

a. Assured Channel. A network communication link that is protected by a security protocol providing authentication and data integrity, and employs DOD-approved cryptographic methods whenever cryptographic means are utilized. Examples of protocols and mechanisms that are sufficient to meet the requirements of authentication and data integrity protection for an assured channel include:

- (1) SIPRNET
- (2) IPSec
- (3) SSL
- (4) Transport layer security (TLS)
- (5) Secure multipurpose Internet mail extension (S/MIME)
- (6) Digital code-signing

b. Trusted Source. A source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication. Examples of mechanisms that are sufficient to validate the identity of a trusted source include:

- (1) Connection via the SIPRNET.
- (2) Digital signature over the mobile code using a DOD-approved PKI code-signing certificate.
- (3) Authentication of the source through a channel authenticated by a trusted source (e.g., DOD PKI or DOD-approved PKI encrypted S/MIME E-mail or SSL server certificate authenticated SSL connection from web server).

c. Mediated Access. Denotes access to system resources subject to the control and approval of runtime-enforced security policy, either during execution or at the beginning of execution. Runtime-enforced security policy provides controlled access to system resources via an intermediary such as an interpreter, virtual machine, or security manager.



d. Unmediated Access. Denotes direct use of system resources, not subject to any approval or control beyond that imposed on conventional-user applications.

e. Code-Signing Certificate. A PKI certificate that can be used to digitally sign code. Such a certificate has a specially assigned attribute (referred to as the *code-signing bit*) set.

f. DOD-Approved PKI Certificate. A PKI certificate issued from a certificate authority approved under DOD PKI policy.

g. Component CIO. The C/S/A CIO.

h. Category 1. Mobile code technologies that provide broad functionality allowing unmediated access to workstation, host, and remote system services and resources. Category 1 mobile code technologies have known security vulnerabilities with few or no countermeasures once they begin executing. They pose a severe threat to DOD operations, and the high risk associated with their use outweighs most possible benefits. The implementations of some mobile code technologies differentiate between signed and unsigned mobile code, and can be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. When Category 1 mobile code is signed with a digital certificate from a trusted source, the risk is somewhat reduced.

(1) Use of Category 1 mobile code in DOD information systems is permitted only when signed with a DOD-approved, PKI code-signing certificate and obtained from a trusted source. In the absence of DOD-approved, PKI code-signing certificates, the responsible CIO may approve the code-signing certificates of other unique code-signing authorities.

(2) When possible, unsigned Category 1 mobile code will be blocked at the enclave boundary, workstation, and applications. Note that blocking at the enclave boundary is not sufficient because mobile code that arrives encrypted (over an SSL connection) or within E-mail cannot be detected or blocked at the enclave boundary. However, the execution of mobile code can usually be disabled in desktop software packages such as browsers, E-mail, and office applications. To the extent possible, all DOD computer systems, workstations, and applications capable of executing mobile code will be configured to block the execution of unsigned Category 1 mobile code technologies obtained from outside the enclave boundary.

(3) In addition, new development or procurement efforts may not include products that contain, use, or depend on the download and/or

execution of unsigned Category 1 mobile code technologies. The DOD CIO and the component CIOs are authorized to grant waivers to permit the use of unsigned Category 1 mobile code technologies in critical situations and in new procurement and development efforts. If the CIO grants a waiver to permit unsigned Category 1 mobile code, the waiver should require the use of a NIAP-approved mobile code security product along with a secure configuration for that product.

i. Category 2. Mobile code technologies that have full functionality allowing mediated or controlled access to workstation, host, and remote system services and resources. They also have known fine-grained, periodic, or continuous countermeasures or safeguards against security exploits. Category 2 technologies pose a moderate threat to DOD information systems. When combined with prudent countermeasures against malicious code and exploitation, their use can afford benefits that generally outweigh the risks.

(1) Category 2 mobile code may be used in DOD information systems if the mobile code is obtained from a trusted source over an assured channel. In addition, unsigned Category 2 mobile code that executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host) may be used whether or not it is obtained from a trusted source over an assured channel. When possible, web browsers and other mobile code-enabled products will be configured to prompt the user prior to the execution of such constrained unsigned Category 2 mobile code.

(2) When feasible, protections against malicious forms of Category 2 mobile code will be employed at end-user systems (hosts and workstations) and at enclave boundaries. If code signing is used to meet the requirement for a trusted source over an assured channel, a DOD-approved, PKI code-signing certificate will be used when available. In the absence of DOD-approved, PKI code-signing certificates, the responsible CIO may approve the use of code signing certificates of other unique code-signing authorities. When SSL is used to meet the requirement for an assured channel, commercial-quality PKI is sufficient.

(3) The responsible CIO may grant a waiver to allow the use of Category 2 mobile code that does not meet the above restrictions (i.e., mobile code not obtained from a trusted source over an assured channel, or unsigned mobile code that does not execute in a constrained environment).

j. Category 3. Mobile code technologies that provide limited functionality with no capability for unmediated access to workstation, host, and remote system resources and services, and have fine-grained, periodic, or continuous

security safeguards against security exploits. Category 3 technologies are of limited risk to DOD systems. When combined with vigilance comparable to that required to keeping any software system configured to resist known exploits, the use of Category 3 technologies affords benefits that generally outweigh the risks. Category 3 technologies may be used in DOD information systems.

k. Emerging Technologies. Any mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet been assessed and categorized into one of the above three risk categories. Because the threat to DOD systems and operations posed by emerging technologies has not been assessed, the risk-versus-benefit calculation cannot be made. Due to uncertain risk, the use of emerging technologies is prohibited unless the DOD or component CIO explicitly grants a written waiver. The download and/or execution of unwaivered emerging technologies will be blocked by all means available at the enclave boundary, workstation, and within applications.

1. Mobile Code in E-mail. Due to the significant risk of malicious mobile code (viruses and worms) downloaded into user workstations via E-mail, the DOD policy for mobile code in E-mail is more restrictive. To the extent possible, the automatic execution of all categories of mobile code in E-mail bodies and attachments will be disabled. Whenever possible, desktop software will be configured to prompt the user prior to opening E-mail attachments that may contain mobile code.

4. Scope. This appendix provides general guidance to assist DOD computer users in configuring their workstations and firewalls to implement DOD mobile code policy.

#### 5. Guidance for Category 1 Mobile Code Technologies

a. Use Category 1 mobile code only when signed with a DOD-approved, PKI code-signing certificate and obtained from a trusted source. In the absence of DOD-approved, PKI code-signing certificates, the responsible CIO may approve the use of certificates of other unique code-signing authorities.

(1) All types of Category 1 mobile code originating from within an enclave boundary may be used within that same enclave boundary (code originating and traveling only within a single enclave boundary is not considered mobile code under this guidance).

(2) Whenever possible, enclave boundaries, workstations, and applications will be configured block the download and execution of unsigned Category 1 mobile code.

(3) Desktop software products should be configured to prompt the user prior to executing signed Category 1 mobile code. When prompted, users must use vigilance to prevent the execution of signed Category 1 mobile code not originating from a trusted source or not signed by an approved certificate.

b. Guidance for workstation products to disable the use of unsigned Category 1 technologies and to enable prompting prior to execution of signed mobile code.

(1) All client desktop software will be configured to disable the download and execution of unsigned Category 1 mobile code and prompt the user prior to downloading and executing signed Category 1 mobile code. For those implementations of Category 1 mobile code technologies that do not differentiate between signed and unsigned mobile code or cannot be configured to only disable unsigned mobile code (e.g., a Netscape ActiveX plug-in or Lotus Notes Browser), disable all mobile code for that implementation.

(2) When it is not possible to disable a Category 1 technology in a workstation product, other countermeasures are required to reduce the associated risk to level acceptable to the DAA for protection of DOD networks (An example includes enabling warnings for mobile code combined with subsequent user action).

(3) Currently, the following mobile code technologies are assigned to Category 1:

(a) ActiveX.

(b) Windows scripting host (WSH), when used to execute mobile code.

(c) Microsoft Disk Operating System (MS-DOS) batch scripts when used as mobile code.

(d) UNIX shell scripts when used as mobile code.

(e) Shockwave movies, including Xtras.

(4) ActiveX is assigned to Category 1 because whether signed or unsigned, ActiveX controls execute with full unconstrained and unmediated access to all system resources. Many, but not all, implementations of ActiveX technologies can differentiate between signed and unsigned ActiveX controls and support disabling of unsigned ActiveX controls while enabling the

execution of signed ones. The ActiveX plugin for Netscape is an example of an implementation that does not differentiate between signed and unsigned ActiveX controls, and hence the ActiveX plugin must be uninstalled and deleted.

(5) Microsoft's WSH is assigned to Category 1 (when used to execute mobile code) because when mobile code executes under it (instead of in the browser) the risk is increased to the Category 1 level. For example, when a Category 3 mobile code script (the VBScript in the ILOVEYOU virus) executes in WSH, the mobile code acquires unmediated and unconstrained access to all system resources. WSH does not differentiate between signed and unsigned scripts. Hence its ability to automatically execute mobile code must be disabled.

(6) Similarly, both MS-DOS batch scripts and UNIX shell scripts execute with full unconstrained and unmediated access to all system resources. MS-DOS batch scripts and UNIX shell scripts that are pre-installed on the user's workstation (autoexec.bat) are not considered mobile code and may be freely used. However, when an MS-DOS batch script or UNIX shell script downloads into the user's workstation as mobile code, it falls under Category 1. Both MS-DOS batch scripts and UNIX shell scripts technologies do not differentiate between signed and unsigned scripts. Hence, the automatic execution of both MS-DOS batch scripts and UNIX shell scripts mobile code must be disabled.

#### 6. Mobile Code in E-mail Messages and Attachments

a. E-mail viruses and worms are forms of malicious mobile code sent to a user via E-mail. As has been recently demonstrated by the ILOVEYOU and TRUELOVE viruses, such malicious mobile code can, when executed corrupt user files, modify the Windows registry, replicate itself by sending copies to everyone in the user's address book, and trash system files requiring a complete reinstallation of Windows. A DOS attack has also been demonstrated using malicious mobile code sent by E-mail.

b. Due to the significant risk of malicious mobile code downloaded into user workstations via E-mail, DOD policy restricts mobile code in E-mail independent of risk category. To the extent possible, the automatic execution of all categories of mobile code in E-mail bodies and attachments will be disabled. Whenever possible, desktop software will be configured to prompt the user prior to opening E-mail attachments that may contain mobile code.

c. Mobile code can be downloaded via E-mail through several different mechanisms. Mobile code can reside in an E-mail body or an E-mail

attachment and downloaded as part of the actual E-mail. Alternately, the E-mail body or attachment can contain HTML or scripts which, when executed, cause mobile code to be retrieved from an external source, downloaded into the workstation, and executed.

d. Most E-mail products have the ability to automatically execute HTML in message bodies and attachments as soon as the user clicks on the message title or views the message body in the preview window (without the user explicitly clicking on an attachment). If an attachment contains HTML that invokes a Java applet, script, or other mobile code, it will automatically download and execute without the user's knowledge (VBS\_KAKWORM virus). HTML that invokes mobile code can also be placed in the message body itself (e.g., BUBBLEBOY virus).

e. An E-mail attachment may contain mobile code scripts (VBScript or JavaScript). When the user clicks on the attachment to open it, the scripts can automatically execute under WSH. When the scripts run in the WSH execution environment, the mobile code receives full unconstrained access to all system resources (ILOVEYOU, TRUELOVE, and VBS\_KAKWORM viruses used this vulnerability). When used in this manner to execute mobile code, WSH is assigned to Category 1.

f. Several countermeasures should be used to protect user workstations from malicious mobile code in E-mail and their attachments (viruses and worms) as required under DOD mobile code policy.

(1) Disable automatic execution of **all** mobile code (e.g., ActiveX, Java, JavaScript, and VBScript) in E-mail bodies and attachments (when possible).

(2) Disable automatic execution of HTML in E-mail bodies and attachments (when possible). This will prevent immediate, automatic execution of HTML that may download and execute mobile code from remote sites when the user previews a message. The user will then be able to safely preview the message, optionally view the page source of suspicious-looking messages, and subsequently decide whether to open the attachment. Note that the user will still be able to intentionally click the E-mail attachment to execute HTML in that attachment.

(3) Enable user prompts prior to opening an E-mail attachment that may contain mobile code. This is done by enabling the "confirm open after download" feature in Windows (and those E-mail products that maintain their own file types) for those file types that may contain mobile code.

(4) Prevent E-mail products from automatically forwarding mobile code in attachments to WSH for execution.

(a) In those E-mail products (Netscape Communicator) that maintain their own associations between file types and applications, disassociate VBScript, JavaScript, and WSH-related file types from the WSH application. This will prevent the E-mail product from automatically forwarding mobile code (scripts written in VBScript or JavaScript) in E-mail bodies and attachments to WSH for execution. Note that the user will still be able to save the attachment in a file and subsequently manually run WSH to intentionally execute any mobile code script in the file.

(b) In Windows, disassociate VBScript, JavaScript, and WSH-related file types from WSH. Some E-mail products, such as Outlook, cannot disassociate file types from applications. Instead, they use the Windows file type associations to select the appropriate application to process a file. Disassociating these file types in Windows will prevent the contents of files with those related file extensions from automatically executing in WSH whenever the user clicks on the file. This will prevent the automatic forwarding and execution of mobile code scripts in WSH for both mobile code in E-mail attachments (for those E-mail products that use the Windows file type associations) and mobile code in a saved file. The user will still be able to manually run WSH to intentionally execute a mobile code script.

(c) Some E-mail products cannot be configured to implement all of these countermeasures. System administrators will implement as many of these countermeasures as possible.

## 7. Guidance for Category 2 Mobile Code Technologies

a. DOD mobile code policy permits the use of all Category 2 mobile code obtained from a trusted source over an assured channel. In addition, the policy permits the use of unsigned Category 2 mobile code that executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host), whether or not it originates from a trusted source over an assured channel.

b. Currently, the following mobile code technologies are assigned to Category 2:

(1) Java applets.

(2) Visual Basic for Applications.

(3) LotusScript.

(4) PostScript.

(5) PerfectScript.

Java applets and LotusScript constrain unsigned mobile code to a sandbox-like environment without access to local system and network resources. Hence, both unsigned Java applets and unsigned LotusScripts are permitted whether or not they originate from a trusted source over an assured channel.

c. The following mechanisms are sufficient to validate the identity of a trusted source:

(1) Connection via the SIPRNET.

(2) Digital signature over the mobile code itself using a DOD-approved, PKI code-signing certificate.

(3) Authentication of the assured channel of the transfer by public key certificate (e.g., SSL server certificate from an SSL web server).

d. The following protocols and mechanisms are sufficient to meet the requirements of authentication and data integrity protection for an assured channel:

(1) SIPRNET.

(2) IPsec.

(3) SSL.

(4) TLS.

(5) Digital code-signing.

e. Not all of the above mechanisms are widely implemented. Given the current state of Internet technology, DOD policy permits the execution of Category 2 mobile code under the following conditions:

(1) Unsigned code that executes in a constrained sandbox-like environment without privileges.



(2) Any code downloaded from the SIPRNET.

(3) Code (possibly executing with privileges) signed with a PKI code-signing certificate approved under DOD PKI policy or by the component CIO.

(4) Originating from a source known and trusted by the user and downloaded over an SSL connection.

f. The use of Category 2 mobile code not obtained under these conditions is permitted only with the approval of the user's component CIO. (Note that Category 2 mobile code pre-installed on the user workstation is not covered by the policy and may be freely used).

#### 8. Workstation Guidance to Disable Category 2 Mobile Code Technologies

a. DOD mobile code policy permits the use of all Category 2 mobile code obtained from a trusted source over an assured channel. In addition, the policy permits the use of unsigned Category 2 mobile code that executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host), whether or not it originates from a trusted source over an assured channel.

b. Paragraph 7 lists the various acceptable mechanisms that may be used to meet the requirements for a trusted source and assured channel; however, not all of these mechanisms are widely used. Given the current state of Internet technology, the policy permits the execution of Category 2 mobile code under the following conditions:

(1) Unsigned code that executes in a constrained sandbox-like environment without privileges.

(2) Any code downloaded from the SIPRNET.

(3) Code (possibly executing with privileges) signed with a PKI code-signing certificate approved under DOD PKI policy or by the component CIO.

(4) Code originating from a source known and trusted by the user and downloaded over an SSL connection.

c. The use of Category 2 mobile code not obtained from such sources and communication channels is permitted only with the written approval of the user's component CIO. (Category 2 mobile code pre-installed on the user workstation is not covered by the policy and may be freely used.)

d. Disabling Category 2 technologies in the workstation for those users that are directed (or choose) to do so.

(1) Users may choose (or be directed) to disable Category 2 mobile code technologies when visiting untrusted web sites, using communication channels that do not meet the above requirements for an assured channel, when operating under high-threat conditions, or when under cyber attack (computer network attack).

(2) If it is not possible to disable Category 2 technologies in a workstation product, other substitute countermeasures are recommended (such as enabling warnings for mobile code and user direction not to execute the mobile code).

#### 9. Guidance for Category 3 Mobile Code Technologies

a. The following mobile code technologies are assigned to Category 3:

(1) JavaScript, including Jscript and ECMAScript variants, when executing in browser.

(2) VBScript, when executing in the browser.

(3) Portable Document Format, or PDF.

(4) Flash animations.

b. These mobile code technologies are low risk and may be freely used in DOD information systems.

10. Emerging Technologies. Emerging technologies are those mobile code technologies that have not yet undergone a risk assessment and been assigned to a risk category. Emerging technologies will not be used in DOD information systems. In critical situations, the C/S/A CIO may grant a waiver to permit the use of an emerging technology.

11. Guidance to Developers on Selection and Use of Mobile Code in DOD Information Systems. The developer's selection of which mobile code to use in developing software ultimately impacts the security of the client workstations. Developers should use the lowest risk mobile code technology that will meet their requirements. For additional guidance refer to DISA's "Developer's Guide for Using Mobile Code Technologies in DOD and IC Information Systems." This guide is available at [www.iase.disa.mil](http://www.iase.disa.mil).

## APPENDIX K TO ENCLOSURE C

## FIREWALL GUIDANCE

1. Background

a. The main function of every firewall is access control, which filters entry in and out of the network based on the security policy of that network or enclave. Some firewalls also offer a function called mobile code blocking. Mobile code blocking allows the firewall to block code such as Java applets, JavaScript, and ActiveX. This function is currently limited and cannot block code that is embedded within objects such as E-mail or HTML documents.

b. A key element of successful IA is employing a layered security strategy to reduce vulnerabilities and defend against a wide range of threats. The DOD philosophy of IA through defense-in-depth responds to this need to distribute security protection at all levels. Currently, the C/S/As are responsible for deploying and configuring firewalls or firewall-like technologies to protect their networks. Under this operational environment, the C/S/As have had to develop their own unique firewall configuration guidance. However, interconnected DOD networks operate in a shared-risk environment and need to meet minimum configuration standards. Without an established firewall-configuration baseline, DOD firewall configurations differ among the various organizations. DOD firewall ports, protocols, and services policy provides configuration settings and countermeasures for the Military Services and DOD agencies to meet the demands of this shared-risk environment. The policy is maintained and updated by the DOD ports and protocols management process. DOD information systems are only as strong as the weakest link. For DOD networks to operate in a shared-risk environment and maintain a level of trust with other Services and agencies standardized firewall deployment guidance and DOD firewall-configuration control process must be developed, implemented, and sustained.

c. The DISA and the NSA have taken the lead on establishing firewall-configuration baselines and creating and maintaining standardized DOD firewall guidance while promoting a common framework for firewall architecture design and a common criteria protection profile. This firewall configuration policy is based on the firewall design philosophy to “deny all services unless expressly permitted.” The policy to “deny all” is stronger and safer than a policy that “permits all services unless expressly denied.” However, the “deny-all” policy is more difficult to implement and may impact

users because many of the desirable services may have to be blocked or more heavily restricted to maintain an appropriate level of security.

## 2. Objective

a. This appendix covers one of the enclave boundary protection mechanisms -- firewalls. The information presented in this appendix establishes basic firewall architectural policy to be used by the C/S/A in support of the defense-in-depth strategy for classified and unclassified systems.

b. The architectural guidance in this appendix encompasses overall DOD firewall architecture deployment strategies. Additional baseline firewall configuration guidance to assist in installation of a firewall in a classified or unclassified network can be found at [http://www.iatf.net/protection\\_profiles](http://www.iatf.net/protection_profiles). Questions on IA and firewalls can be obtained through the DISA information desk at <http://matthe.iiie.disa.mil/iaseinfoesk.html>. In addition, this appendix describes firewall types, assurance levels, firewall services, and potential threats.

3. Security Policy. One of the primary functions of a firewall is to support and implement an organization's security policy. Each C/S/A will support development of a common DOD baseline ports and protocols security policy to ensure that common DOD security and interoperability requirements as well as individual C/S/A needs are met. The firewall-related security policy, as a minimum, identifies:

- a. All firewall protected network assets.
- b. All firewall protected network support systems and services.
- c. All network system support services and systems criticality.
- d. Threats.
- e. Mitigation measures.
- f. Required audit items.
- g. Incident response procedures.
- h. Manager, administrator, and user responsibilities and training requirements.

4. Firewall Implementation. Firewall implementation should include coordination with the supporting Service network operations center and CERT/CIRT as well as DOD GNOSC and CERT.

5. Firewall Security Requirements

a. The firewall will be located in a physically secure location. Firewalls will be certified against the CC to the appropriate EAL level.

b. For all software based firewalls, underlying OSs will be hardened prior to loading the firewall in accordance with most recent NSA and DISA guidance pertaining to the particular OS. For example, refer to "Guide to Securing Microsoft Windows NT Networks," September 6, 2000, Version 4.1 prepared by the Network Attack Techniques Division of the Systems and Network Attack Center or more current versions. To obtain a compact disk, call the NSA IA Service Center at 1-800-688-6115. Also see "Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000, " Version 2, Release 1, December 31, 2001.

c. The firewall and any corresponding OS will be kept up to date with the most current approved patches and other bug fixes and will have current maintenance contracts for both the hardware and software. Patches and bug fixes should be obtained through DOD channels and in coordination with configuration control. Installation of patches and bug fixes should be compliant with IAVAs and Service equivalent directives.

d. Firewalls will employ network address translation (NAT) to hide internal IP addresses to the maximum extent possible. Configure NAT firewalls so that outbound traffic appears as if the traffic had originated at the firewall. Any exceptions will be applied on a case-by-case basis and must be fully documented.

e. Source routing on the firewall will be disabled.

f. All traffic on the firewall's external interface that appears to be coming from internal network addresses will be rejected. These measures are referred to as "anti-spoofing" or "ingress and egress filtering."

g. All factory default account names and passwords will be changed. All accounts that are not required will be removed. Default protocol and application settings will be changed, such as: secure socket layer certificates for applications like secure socket shell (SSH) or secure remote administration and simple network management protocol read/write community strings.

h. Disable any capability or feature not specifically required for firewall operation. This should eliminate exposure to possible security vulnerabilities.

i. The firewall should reboot to a known configuration to prevent attacks that involve configuration change and reboot.

j. Store system configuration information on read-only media or on off-line storage. Store backup media at an off-site storage location.

k. Firewall will only contain software or files directly related to the functioning firewall. No general-purpose computing capabilities or development tools shall be installed unless specifically required for firewall operation. The firewall will not be a host for public data. Remove unnecessary compilers, editors, and other program development tools not specifically required for firewall operation, since they could be used to install or execute hostile code such as Trojan Horses or backdoors.

l. The number of firewall accounts will be limited to only those absolutely necessary for proper operation. Changes to, access control lists, services, filters, or proxies will first be coordinated with and approved by the policy-making firewall authority.

m. Upon availability of capability, the firewall will uniquely identify and authenticate the claimed identity of a user before granting access to the firewall's administration interface. Authentication (token, smart card, or PKI certificate) will be required for all firewall management. Develop migration plans to bring all firewalls into compliance within 12 months after technology availability. Although remote administration is discouraged, if required, remote management sessions will be conducted through a secure transport (SSL, VPN/IPSec) from trusted management terminals within a protected network, including remote protected networks. All authentication will be PKI enabled by July 2003. As a goal, management protocols will be encrypted and authenticated using unique, Internet Assigned Numbers Authority-listed, TLS protected TCP ports. No unsecure remote management sessions are authorized.

n. The firewall must provide an accurate readable audit trail of security-related events, with correct date and times, and a means to search and sort the audit trail based on relevant attributes. The goal is to record relevant security events including all administrators' activity, successful and unsuccessful authentication attempts, and any activity caught by the firewall "deny all rule." Audit logs will be reviewed daily. The firewall will provide a means to immediately notify the administrator of any high-priority security relevant events (such as excessive failed login attempts) or critical operational events

(such as near full audit records). Where possible, audit logs will be stored on an external dedicated audit server on the protected network. Access to the audit server will be limited to the minimum number of authorized personnel required to perform the function. The local IA office will provide guidance on the of time audit records will be maintained, but audit records should be maintained for a minimum of 6 months. Audit logs should be written to “write-once” media.

o. Firewalls should be configured to provide individual authentication as well as IP address authentication that restricts traffic to source and destination.

p. The firewall will prevent the re-use of authentication data for administrators attempting to access the firewall.

#### 6. Configuration Management, Maintenance, and Testing of Firewall

a. Baseline firewall configuration will be mapped against approved security policy.

b. Perform installation verification testing to validate that components were properly entered when the firewall was installed. Results will be documented and kept on file for reference.

c. A vulnerability scanner will be run against the firewall and reported vulnerabilities will be corrected prior to connecting the firewall to the “live” network. Once a satisfactory (i.e., corrected vulnerabilities with acceptable residual risks) scan has been completed. The output should be securely stored for future reference and comparison.

d. Vulnerability scans will be conducted at least quarterly as part of routine maintenance. Vulnerability scans should be conducted against hosts internal to the firewall, in addition to firewall itself, to confirm an adequate security policy is being enforced.

e. Regular upgrades and updates to the vulnerability scanner will be maintained to ensure that current vulnerabilities have been incorporated.

f. The host network SSAA system architecture description section will clearly identify the firewall location(s), services, and exact functions. In addition, the SSAA will include plans for certification and recertification, auditing of logs, and policies for identifying and authenticating approved administrators.

g. Because the firewall is a key component of a network defense posture, there should be at least one (1) cleared, qualified firewall administrator assigned. A firewall administrator should be available for emergency changes in response to computer network events and incidents.

h. Firewall upgrades and updates will be documented and coordinated through the configuration management process.

i. The firewall will be tested and shown to be resistant to potential attackers.

j. An annual review of all firewall rules will be conducted.

## 7. Scope

a. The architecture and configuration guidance in this appendix applies to the Joint Staff, the Services, the combatant commands, the Defense agencies, DOD field activities, and other activities when engaged in direct support of DOD missions. This appendix applies to the DOD sustainment base and deployed tactical force(s). Tactical deployment does not negate the need to implement basic security concepts; if anything, it increases that need. Planning for the use and configuration of firewalls to protect tactical systems must be an integral part of contingency planning for all deployments.

b. The architecture and configuration guidance in this appendix assumes that the DOD Service or agency has the knowledge to perform firewall software and hardware installation and associated network connectivity. This appendix addresses different target environments, best types of firewall technologies suited for a particular environment, and the required assurance level. This information is presented in the context of case-specific firewall deployment guidance, configuration guidance, and interoperability requirements based on the network classification level.

c. Firewall architectures and configurations presented in this guidance document should be implemented as funding is available, the cyber threats and vulnerabilities to DOD IT are such that implementation should begin immediately when possible. As systems are upgraded and funding becomes available, the architectures and configurations presented here must be recognized as an urgent priority and implemented as soon as possible.

d. Updates to specific configuration guidance will be posted as required on the IATF website at [http://www.iatf.net/protecton\\_profiles/firwalls.cfm](http://www.iatf.net/protecton_profiles/firwalls.cfm). Additional information is available at <http://mattche.iiie.disa.mil/iaseinfoDesk.html>. NSA guidance on configuring



routers can be found at [www.nsa.gov](http://www.nsa.gov) under "Security Recommendation Guides." In addition, NSA guidance for securing Microsoft Windows NT networks and applications can be obtained by calling 1-800-688-6115. For NSA information on securing UNIX networks contact 410-854-6526. DISA's STIGs on securing enclaves, networks and operating systems can be <https://iase.disa.mil> and <http://iase.disa.smil.mil>. Firewalls and routers fundamentals, an interactive, multimedia web based training and computer based training product for Level 1 system administrators, provides a high-level overview of security issues related to the use of firewalls and routers. For access to guides or for additional STIG information contact the Field Support Office Support Desk, 717-267-9284

## 8. Overview

a. Boundary-protection devices such as firewalls restrict access to an internal network. Specifically, a firewall protects a trusted network from an untrusted network. Typically, the two networks involved are an organization's internal trusted network and an untrusted network (the NIPRNET, other DOD enclave with a different security policy, Internet or a network with a lower classification).

(1) For a firewall to be effective, incoming and outgoing traffic across the trusted network must pass through the firewall or equivalent packet filter and/or proxy, which permits only authorized traffic to pass, as stipulated in the network's security policy. Because the firewall becomes the only access point to the network, it facilitates centralized enforcement of the security policy. By serving as the only direct path to the network, the firewall limits the vulnerability of the network to attacks. The disadvantage, however, is that as the only entrance, the firewall becomes a bottleneck and the biggest target for attacks on the network. Additionally, tunneling techniques can bypass firewall security and IDSs and open networks to possible compromise. Care must be taken when tunneling through systems to ensure only appropriate ports, protocols, and authorized addresses access internal hosts and all traffic is monitored by an IDS.

(2) A firewall protects against attacks by denying unauthorized traffic while allowing authorized traffic onto the network.

(a) A firewall, when properly configured according to DOD security policy, provides protection from unauthorized access by prohibited addresses and traffic types. This ensures that protected systems and networks maintain availability and are defended against attacks.

(b) Firewalls also provide a risk-managed method of filtering essential data traveling across the network. A firewall must effectively implement several functions to provide adequate security.

(3) Auditing is an important function of firewalls. To audit, firewalls log activity between networks and can automatically notify an administrator of events such as unauthorized activity. Many current firewalls can also provide NAT, which hides the IP addresses of the internal network. As stated earlier, the firewall is the main point of access to the internal network. Therefore, the firewall ability to authenticate connections and resist attack is one of the most critical functions.

b. When configuring a firewall, determining which services to deny and which to allow is key. These determinations should follow the DOD component and local security policy.

(1) Firewalls must protect against a variety of attacks.

(a) Network-based attacks consist of outside attacks and close-in attacks, in which an attacker, possibly an insider, gains access at a point inside the network. Network attacks include attempts to evade or break down security features, inserting malicious codes, stealing or modifying data, or entering disguised as an authorized user.

(b) Passive intercept attacks consist of monitoring and/or sniffing traffic in and out of the protected network for unprotected communications, weakly encrypted data, and user names and passwords.

(c) Insider attacks are the hardest to protect against. These include authorized users who attempt to steal or modify data or deny access to other authorized users. Insider attacks also include authorized users who inadvertently pose security threats due to lack of knowledge or carelessness.

(2) This appendix only discusses recommended guidance for firewalls. It does not take into account the other necessary layers of security needed for defense-in-depth concept such as intrusion detection (see Appendix N of this Enclosure, "Intrusion Detection") or virus scanning at <http://www.disa.mil/infosec/iaweb/default.html>.

9. Firewall Technology Types. The common types of firewalls are packet filtering, stateful inspection, proxy-based or application gateways, circuit gateways, and hybrids.

a. Packet Filters

(1) Packet-filtering firewalls (also known as screening routers) commonly operate at the network layer (open systems interconnection (OSI) layer 3).

(2) Typically, they can filter packets based on host and destination IP address, port number, interface, and direction.

(3) This type of firewall is generally inexpensive, fast, and transparent to the user. However, screening routers do not have a robust auditing capability, nor do they allow the use of strong authentication on incoming connections.

(4) Packet filters are an integral part of the other forms of firewalls that have expanded capabilities. Even so, most of the packet filtering should occur at the screening router.

b. Stateful Inspection

(1) Stateful packet-filtering technology provides an enhanced level of security compared with the static packet filtering described above.

(2) The stateful packet filter looks at the same headers as packet filters. More importantly, this technology allows the firewall to dynamically maintain state and context information about past packets. Security decisions can then be based on this state information.

(a) For example, the firewall can respond to an FTP port command by dynamically allowing a connection back to a particular port.

(b) For that reason, they are advertised as offering greater flexibility and scalability.

(3) Stateful packet-filtering technology also allows for logging and auditing and can provide strong authentication for certain services.

c. Proxy-Based or Application Gateways

(1) Proxy services are specialized application programs that run on a firewall host, often called an application gateway.

(2) Application gateways are generally dual-homed (packet-filtering firewalls can also be dual-homed), which means they are connected to both the protected network and the public network. However, they can be used in other configurations as discussed below.

(3) The firewall mediates access between the two networks via proxies, which are customized for the service each is intended to provide.

(a) Proxy-based firewalls can implement more complex access control policies by providing refined filtering capabilities.

(b) Application gateway firewalls provide detailed logging capabilities and support the use of strong identification and authentication for certain services.

(c) These firewalls are limited in the services available depending on the availability of proxy software.

(d) If these types of firewalls are used at the perimeter, the internal Security Domains must be protected by an application level firewall that meets the enclave requirements.

d. Circuit Gate. A circuit gateway, unlike an application gateway, completes a connection between a client and server without interpreting the application protocol. Therefore, a circuit-level proxy, acting as a wire, can be used across several application protocols. These firewalls are less commonly used because client modifications are likely to be necessary to use the circuit-level protocol.

e. Hybrid. Hybrid systems can use any combination of firewall types and capabilities, for example, combining a proxy-based or application gateway firewall and a packet-filtering firewall's capabilities. Combining these two systems would give you pack-filtering capability (host and destination IP address, port number, interface, and direction filtering) and proxy-based or application gateway capabilities (more complex access control policies with refined filtering capabilities, more detailed logging and stronger identification and authentication for certain services). Due to the addition of the application gateway or proxy abilities, this system would not run as fast as a regular pack-filtering firewall since some speed is sacrificed for increased capabilities that require more processing time.

10. Example Firewall Architectures. The following sections present four different firewall architecture scenarios that can be implemented to protect an enclave (basic filter, dual-homed, screened host, and dual-homed with screened subnet). Although these configurations can be set up in a number of combinations to create hybrid solutions, the focus here will be on these four most common architectures.

a. Basic Filter (Screening Router)

(1) The basic filter setup shown in Figure C-K-1 involves using a router (which can filter inbound and outbound packets on each interface) to screen access to one or more internal servers. This server is the starting point for all external connections. Internal clients who wish to access the external network may do so via this screened server. This configuration can also be setup so clients on the internal network access the router directly via access control lists (ACLs) or IP filtering instead of traversing the screened server.

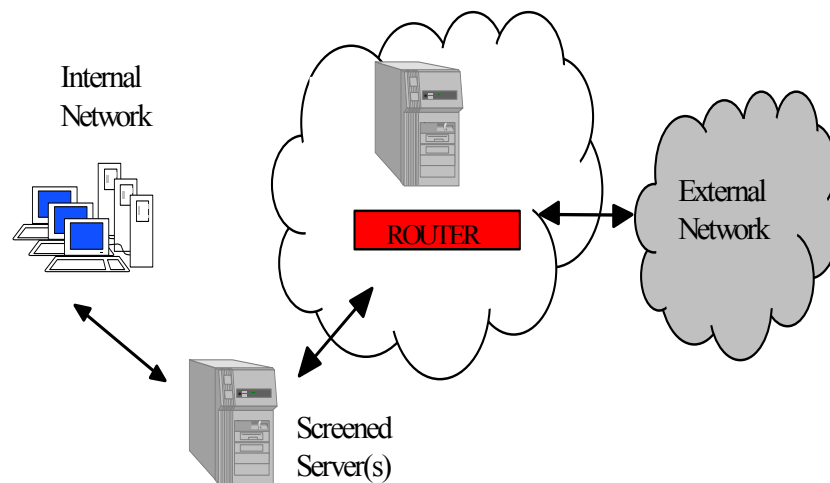


Figure C-K-1. Basic Filter (Screening Router)

(2) Although the basic filter may be one of the cheapest solutions for an organization, it is not recommended for DOD connections to external enclaves (i.e., the NIPRNET, SIPRNET, or JWICS). Setting up a router by itself with ACLs or IP filtering should only be done to protect connections between trusted networks within an organization's enclave boundary.

(3) If basic screening router provides no network address translation functions. The internal users cannot be held accountable for their actions, and the internal IP addresses are passed to an external network. In this case, the

architecture is not a viable solution for protecting an enclave from an untrusted external source.

b. Dual-Homed

(1) The classic dual-homed firewall architecture, Figure C-K-2, is where a host is setup as a gateway with two network interface cards (NIC), one connected to the external network through a router and one connected to the internal network. Packet forwarding is disabled on the gateway, and information is passed at the application level. The gateway can be reached from both sides, but traffic cannot directly flow across it.

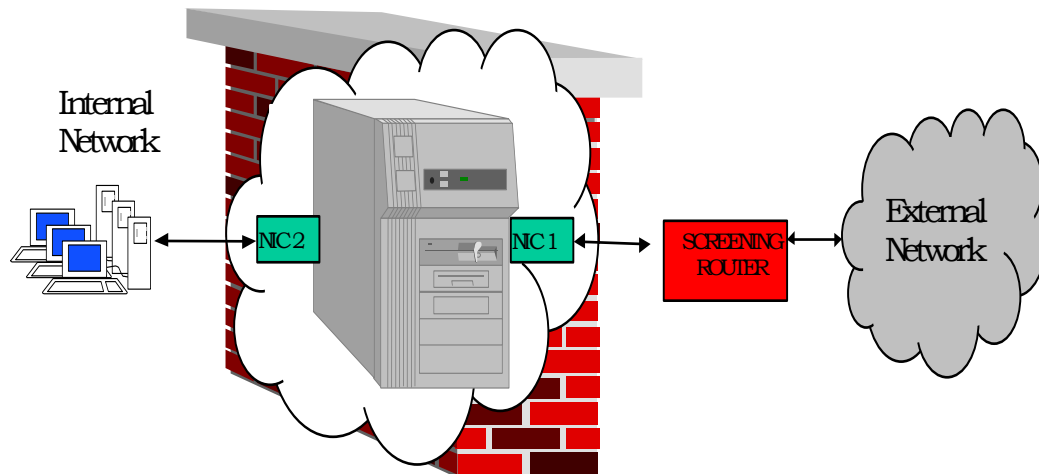


Figure C-K-2. Dual-Homed

(2) The router should also be setup with ACLs or IP filtering so connections are allowed between the router and the firewall only. Some of the disadvantages of using a dual-homed host for a firewall are that it cannot forward packets, thus requiring proxy services that must be configured manually, and performance is limited since all network traffic must pass through one machine. On the other hand, today's dual-homed firewalls offer quite a bit more functionality than the basic filter such as thorough auditing, virus scanning, and VPNs.

(3) The dual-homed architecture is a common choice for some organizations. When performance is an issue, more than one firewall can be implemented in a parallel configuration between the internal and external networks. This design may be implemented, for example, between an organization's SECRET enclave and the SIPRNET. It is recommended that the enclave not provide any web services to the SIPRNET with this architecture in place. The dual-homed with screened subnet is the recommended configuration for providing the web services discussed.

c. Screened Host. This variation of the basic filter shown in Figure C-K-3 involves the use of two filters, the additional filter being used between the screened host and its clients. The “protected” host is known as a bastion host. It provides additional protection in comparison to the basic filter configuration, but still lacks the auditing and address translation functions provided by a full-blown firewall. This architecture could be used to isolate a sensitive subnet from the rest of the enclave, but should not be used to protect the boundary from external sources.

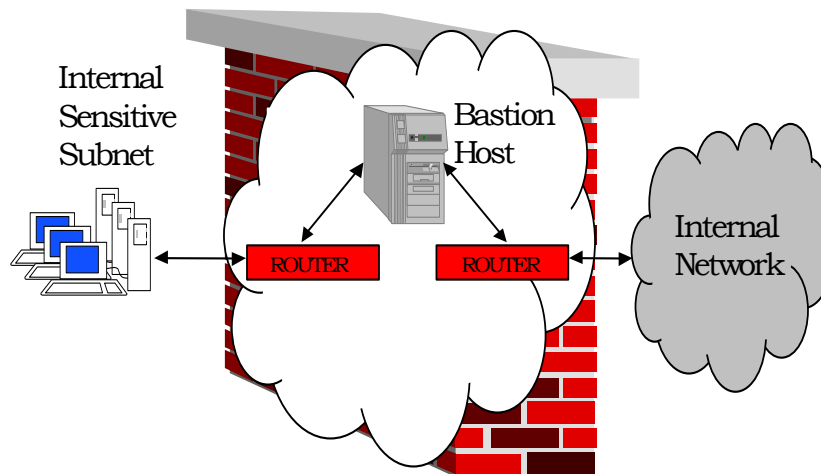


Figure C-K-3. Screened Host

d. Dual-Homed with Screened Subnet

(1) In the dual-homed with screened subnet firewall architecture, Figure C-K-4, a host is set up as a gateway with three NICs, one connected to the external network through a router, one to the internal network, and one to the DMZ. Packet forwarding is disabled on the gateway, and information is passed at the application level or the network layer depending on the type of firewall used. The gateway can be reached from all sides, but traffic cannot directly flow across it unless that particular traffic is allowed to pass to the destination it is requesting.

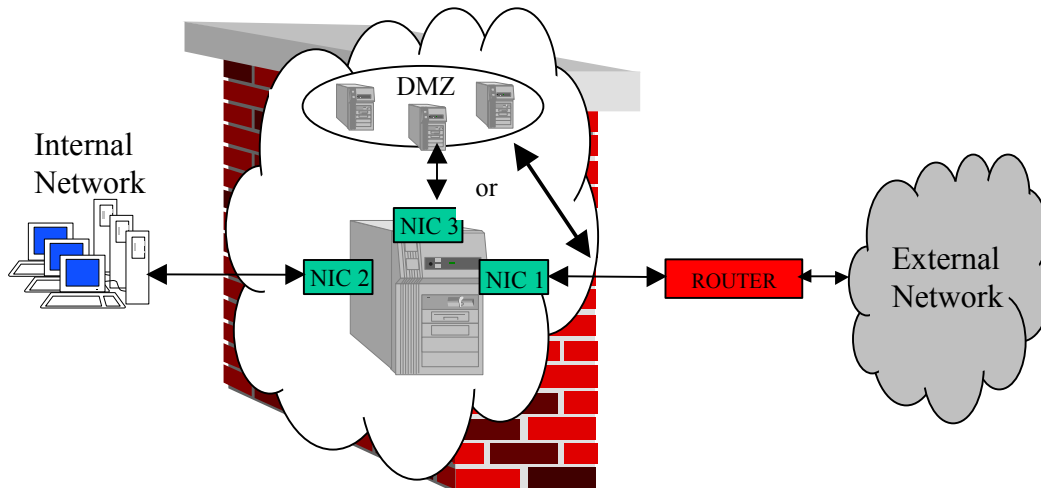


Figure C-K-4. Dual-Homed with Screened Subnet (DMZ)

(2) The router should also be setup with ACLs or IP filtering so connections are allowed between the router and the firewall only. This configuration has some of the same disadvantages of the regular dual-home architecture. However, the screened subnet provides external, untrusted networks restricted access to the DMZ for services such as World Wide Web or FTP. It allows the enclave to place its public servers in a secure network that requires external sources to traverse the firewall and its security policy to access the public servers, but will not compromise the operating environment of the internal networks if hackers attack one of the networks.

(3) The dual-homed with DMZ architecture is a common choice for most organizations that require a public web server. When performance is an issue, more than one firewall can be implemented in a parallel configuration between the internal and external networks.

## 11. Firewall Placement

a. A firewall can be placed at several locations to provide protection from attacks. Each implementation will differ depending on several key factors, including the sensitivity of the networks, the network infrastructure, and the type of network traffic. Usually firewalls are used to protect the boundaries of a network, although at times they can be used to secure a sensitive part of an enclave from the rest of the enclave.

b. There are three main points at which a firewall can be implemented within a network, at LAN-to-WAN/WAN-to-LAN connections, at LAN-to-LAN connections, and at WAN-to-WAN connections.



25 March 2003

(1) LANs and enclaves can be classified as TOP SECRET, SECRET, SBU, and UNCLASSIFIED.

(2) WANs also have different classification levels such as JWICS (TOP SECRET/SCI), SIPRNET, NIPRNET, and public or Internet.

(3) An example of a LAN-to-WAN connection could be an unclassified enclave with a connection to the Internet.

(4) A LAN-to-LAN connection could consist of an SBU LAN interconnecting to another SBU LAN within the same enclave to allow information sharing.

(5) A WAN-to-WAN connection could be the NIPRNET WAN connecting to the Internet.

c. All of these connections are boundaries where firewall capabilities are required to ensure the confidentiality, availability, and integrity of the resources within that boundary.

12. Firewall Functions. The firewalls on the market differ from each other in many ways, but they all have similar, specific functions used to protect boundaries. Different boundary points require different levels of protection; therefore, different functions and different firewalls will be required for each unique connection type. The following describes the various functions that firewalls can serve. It should be pointed out that not every firewall has all the functions discussed below.

a. Access Control and Filtering

(1) Access control and filtering is the main function of every firewall. This function can be accomplished in several ways ranging from a proxy at the application layer of the OSI model to stateful inspection at the Transport layer. By its nature, the firewall implements a specific network security policy that corresponds to the level of sensitivity of the boundary it is protecting.

(a) The main fundamental purpose of the security policy is to limit access to the internal network from external sources. Only necessary inbound connections and services should be allowed.

(b) The firewall also restricts the connectivity of internal users to external destinations. Although internal users are generally trusted, they should be limited in what services they can use through the firewall so that they cannot unintentionally open security vulnerabilities.

(2) The different firewall technologies offer different granularities of access control. Some firewalls are now capable of what were traditionally guard-like filtering functions. For example, firewalls incorporate software that filters access to either specific URLs or categories of URLs. Certain FTP commands can be filtered while other commands are allowed through the firewall. Technology will continue to develop in this area, and very sophisticated and highly refined access-control capabilities are likely to become standard firewall features.

b. Identification and Authentication. Identification and authentication are major functions provided by the different firewall products. While users on the inside of a firewall are often considered trusted, typically, external users who require access to the internal network must be authenticated.

c. Encryption

(1) Encryption in firewalls can be used to provide a private, secure management pathway so that remote management of the firewall is possible. Remote management also requires strong authentication to ensure that the connection comes from a trusted source and the data remains confidential. Remote management will be restricted to authorized individual administrators and requires NSA-approved NIST/FIPS 140-2 (reference aaa)-validated cryptographic protection.

(2) In addition, encryption capabilities in firewalls are used to establish VPNs. A VPN essentially carves out a private passageway over the Internet. The use of VPNs is growing primarily because of interoperability issues. Implementation of IPSec protocols (the protocols advocated by IPv6 to establish VPNs) have been quite complex. Firewalls also widely offer support for SSL and SSH, security protocol that provides communications privacy (confidentiality) over the Internet.

d. Auditing

(1) Auditing is a critical component of firewalls. The firewall provides an ideal place to log all of the activity going on between networks.

(a) Most firewalls log the time, type of service, and source and destination ports of incoming packets. Some firewalls allow the selection of certain events to be logged. Firewalls can provide for automatic notification of the administrator via pager or E-mail depending on the type of access attempt.

(b) In some cases, the firewall can then attempt to trace future attempts at access to gain more information about the attacker. When subjected to various DOS attacks, some firewalls can either deny packets to guard against the attack or shut down entirely. Despite these advances, current firewall technology falls short in the area of reporting and alerts associated with the log files.

(2) As firewalls continue to incorporate more capabilities, the complexity of the product increases, thus increasing the number of avenues for attack.

e. Virus Scanning

(1) A few firewalls offer virus-scanning software on the firewall itself, mainly through vendor partnerships. Scanning for viruses on the firewall is difficult simply because of the large number of viruses that have been identified and the number of file formats that carry viruses is far too numerous to scan at the firewall. In addition, to be effective, the firewall antivirus capability must be updated regularly to reflect the additional viruses discovered. Probably the biggest major obstacle to performing virus scanning on the firewall is the resulting reduction in performance. This however, can be remedied by using multiple firewalls running in parallel configurations.

(2) Some networks do overcome this obstacle by scanning for viruses entering the network using a separate dedicated virus-scanning machine. Virus scanning at the network boundary provides a first line of defense and can be used in combination with an organization-wide program for virus scanning at the desktop.

f. Network Address Translation

(1) The majority of firewalls available on the market today provide for NAT. NAT is a means of hiding the IP addresses on the internal network from external networks. The need for IP address translation arises in two cases:

(a) The network administrator wishes to conceal the network's internal IP addresses from the Internet.

(b) The internal network's IP addresses are invalid Internet addresses.

(2) This technology provides advantages in security by hiding the internal network, and its operational capability, by giving the administrator a larger available IP addressee block.

g. Protection Against Attack. Another important aspect of a firewall is how well it protects itself against attack. The firewall itself should be resistant to penetration to assist in preventing hackers from breaking through the firewall and accessing the entire network. Most firewalls run on stripped-down and hardened versions of standard OSs. (Unnecessary executables, compilers, and other dangerous files are removed and unnecessary services are turned off.) In addition, some firewalls employ technology that makes it extremely difficult for a hacker to penetrate the firewall OS. These firewalls are built on trusted OSs or use mechanisms such as type enforcement to provide extra protection against penetration. These types of additional safeguards are traditionally found on guard devices and are beginning to be commonly available on firewalls.

h. Administration

(1) Properly configuring firewall components is critical to network security. Most firewall vulnerabilities arise from improper configuration and maintenance.

(2) Examining the administrative interface provided by the firewall is important. A user-friendly interface will not make the firewall any more secure; however, a well-designed interface can ease the administrative burden and show how well the firewall has implemented the security policy.

(3) Firewalls also use various self-monitoring tools. These tools can provide additional access controls, increase its auditing capability, and provide integrity checking on the file system. Some of these tools are proprietary and are provided with the firewall; other tools are available from open-source code and can be used to enhance firewall security. Open-source code must be certified safe before it is used as part of DOD firewall software.

13. Potential Attacks. The following paragraphs discuss, at a high level, attacks on a LAN or workstation that exploit vulnerabilities in the system's electronic connections. Network-based attacks primarily applicable to the protection for network access (PNA) category of the IATF (reference ggg) are listed below. The other attack categories listed are not directly addressed within the PNA section of the IATF, but relate to the technologies discussed here.

a. Passive Intercept. These attacks are based on such methods as monitoring and/or sniffing unprotected (plain text) communications, decrypting weakly encrypted communications, capturing ID numbers and passwords, and traffic analysis.

(1) Monitoring plain-text transmissions is one common way in which attackers capture data.

(2) Decrypting weakly encrypted traffic is another way that an unauthorized user can gain access to information. Recent reports show that crypt-analytic capability is available in the public domain, as witnessed by the June 1997 collaborative breaking of the 56-bit strength data encryption standard (DES). Although the near-term threat to large volumes of traffic is uncertain, given the number of machines and the hours that would be required to decrypt the information, breaking the 56-bit DES does show the vulnerability of individual transactions.

(3) "Password sniffing" uses protocol analyzers to capture passwords.

(4) Traffic analysis requires a great deal of time and patience and only a small amount of technology.

(a) Observation and analysis of external traffic patterns, even without decryption of the underlying information, can give critical information to adversaries (for example, observation and analysis of the extension of a network into a tactical theater of operations).

(b) Changes in traffic patterns may provide indicators of imminent offensive operations. Observation and analysis of these changes would enable correlation of this activity to real-world events and result in forecasting abilities that would eliminate the element of surprise.

(c) Another use of traffic analysis can be to identify networks processing information from critical-sensor platforms. In this case, probing the sensor and observing resulting traffic patterns can give away sensor response times and sensor sensitivity.

(d) Passive observation of network operations can warn adversaries of impending actions.

1. These warnings may include indications of the end parties in an information exchange, a change in the volume of traffic or traffic patterns, or the timing of information exchanges in relation to external events.

2. Passive observation attacks involve passive monitoring of communications sent over public media (e.g., radio, satellite, microwave, and public switched networks).

(5) Countermeasures for such attacks include use of protected networks, strong encryption of sensitive data, and use of protected passwords or public keying techniques.

b. Network-Based

(1) Network-based attacks include attempts to circumvent or break security features, introduce malicious code (such as computer viruses), or steal data.

(2) Such attacks can include attacks mounted against the network backbone, exploitation of data in transit, electronic penetration into an enclave or LAN through boundary-protection devices (including an enclave's remote-access entry point), and attacks on an authorized remote user when the user attempts to connect to the enclave.

(3) A typical countermeasure against network-based attacks is strong enclave boundary protection. The majority of attacks that occur at the enclave boundary follows.

(a) Modification of Data. Modification of data in transit is one common type of network attack. Such attacks can have far-reaching and disastrous results. For example, in the financial community, it could be devastating if electronic transactions could be modified to change the amount of the transaction or redirect the transaction into another account.

(b) Exploiting the System

1. Exploiting system application and OS software is another common, if not the most common, way that hackers gain access to enclaves. Well-known attacks involve sendmail and X-Windows server vulnerabilities. Recently, there has been a proliferation of alerts regarding Windows 95, 98, ME, NT, and 2000 vulnerabilities. New vulnerabilities in various software and hardware platforms are discovered almost daily. An IAVA is generated whenever a critical vulnerability exists that poses an immediate threat to the DOD (see Appendix A to Enclosure B, "Information Assurance Vulnerability Management Program").

2. An attacker can exploit host or network trust by manipulating files that facilitate the provision of services on virtual and/or remote machines. Well-known attacks involve ".rhosts" that facilitate workstations sharing of files and services across an enterprise network. With this method, an attacker could gain execution access to a user's system commands through a previously identified vulnerability and then use that

access to insert malicious code, such as Trojan horses, trapdoors, viruses, or worms.

3. An attacker can exploit weaknesses in protocols to spoof users or reroute traffic. Well-known attacks include spoofing domain name servers to achieve unauthorized remote log-in, and bombing using the internet control message protocol to knock a machine off the air. Other well-known attacks of this type are source routing to impersonate a trusted-host source, TCP sequence-guessing to gain access, and TCP splicing to hijack a legitimate connection.

4. DOS and distributed DOS attacks are extremely common and highly effective, as evidenced by the attack that took Yahoo.com and other web pages off-line for several hours on 8 February 2000.

(4) The above attack types are those most commonly used by the hacker community. However, they are by no means the only types of attacks that can occur, and new attack methods are invented almost daily.

c. Insider

(1) In this type of attack, the person is either authorized to be within the physical system boundaries or has direct access to it. There are two types of insider attacks: malicious and nonmalicious (through carelessness or ignorance of the user).

(2) The nonmalicious user case is considered an attack because of the security consequences of the user's action.

(a) Although this document emphasizes protecting the "inside" from a potentially hostile outside world, mechanisms are needed for protection from inside intruders also.

(b) Further, once an outsider has successfully attacked a system to obtain access, the outsider in effect becomes an insider, with all the privileges of the component account, maneuvering within the system as any other insider would. Thus, technologies designed to detect attacks by an insider may in fact be used in a similar manner to detect outsider attacks.

25 March 2003

d. Distribution. Hardware or software modification in transit could be the first step in an adversary attack that eventually causes the system to send data or allow unauthorized access, via standard network communications lines.

e. Other. Physical intrusion or hardware or software modification at any point in the life cycle, and the introduction of malicious code via disk, represent additional paths for gaining unauthorized access to the LAN or workstation. Each of these methods can also be a first step in an attack.



## ANNEX A TO APPENDIX K TO ENCLOSURE C

## ROBUSTNESS

1. Robustness Strategy. A robustness strategy is an integral part of determining recommended strength and degree of assurance of proposed security services and mechanisms that become part of a solution set. The strength and assurance features serve as a basis for selecting enclave boundary protection mechanisms; in this case, firewalls. This annex provides guidance for determining the recommended strength and assurance levels for deploying firewalls across the Department of Defense.

2. Determining the Degree of Robustness

a. This is the level of strength and assurance recommended for potential security mechanisms. To determine this level for a given firewall, the customer must consider the value of the information to be protected (in relation to the operational mission) and the perceived threat environment. To aid the customer in determining a site's degree of robustness requirement, the case-solution matrix found in the NSA DOD firewall guidance series (reference fff) was developed. The case-solution matrix is based on NSA protection profiles, which take into account threat levels and value of information levels to identify degrees of robustness needed for specific system mission categories. Consequently, the customer does not have to consider a site's threat level or value of information when the case-solution matrix is used.

b. It should be noted that the robustness strategy focuses specifically on individual security services and mechanisms. The actual robustness of an overall network solution will need to take into account individual solutions. It must consider the implications of composing layered mechanisms and also incorporate an overall assessment of vulnerabilities and residual risks. This annex is dedicated to assisting sites in determining an appropriate firewall configuration. To select which firewall configuration is appropriate for the site-specific firewall, refer to the diagram below, Figure C-K-A-1, and the written description that follows the chart.

C-K-A-1

Annex A  
Appendix K  
Enclosure C**FOR OFFICIAL USE ONLY**

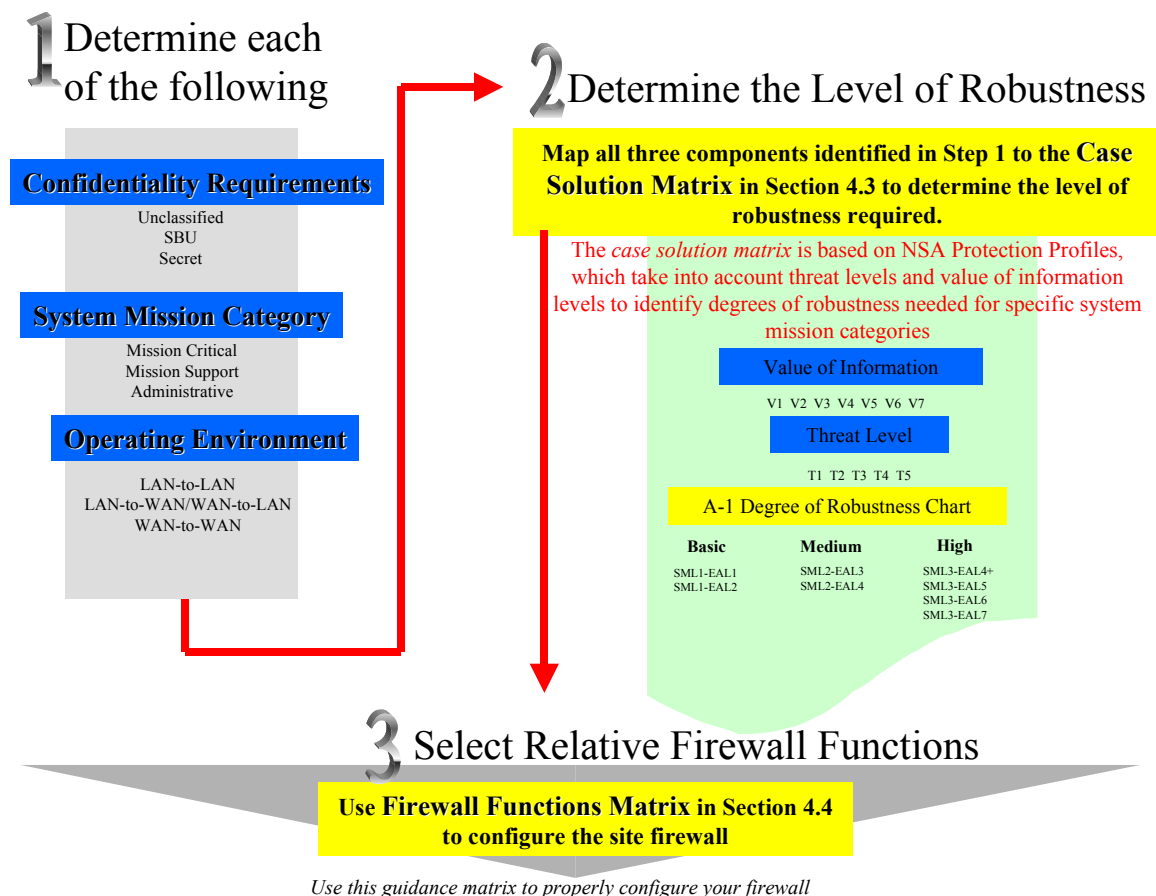


Figure C-K-A-1. Determining the Level of Robustness Flow Chart

c. To determine the needed level of robustness, follow these steps:

(1) Step 1. Identify the enclave the site desires to protect. Then identify the enclave confidentiality requirements, system mission category, and operating environment. (Note: Explanations of each of these are supplied in NSA DOD firewall guidance series (reference hhh) and Appendix A of the series. The available choices per section are listed below.

(a) Confidentiality Requirements – UNCLASSIFIED, SBU, SECRET, or TOP SECRET (TOP SECRET guidance is not available at this time). Note: Because SBU includes Privacy Act and OPSEC data, "UNCLASSIFIED" as identified here is rarely appropriate.

(b) System MAC -- MAC III, MAC II, and MAC I.

C-K-A-2

Annex A  
Appendix K  
Enclosure C

**FOR OFFICIAL USE ONLY**

(c) Operating Environment [network topology] -- LAN-to-LAN, LAN-to-WAN/WAN-to-LAN, and WAN-to-WAN.

(2) Step 2. Once all of the above information is identified, use the case-solution matrix in Section 4.3, NSA DOD firewall guidance series (reference hhh) to determine the appropriate confidentiality requirements in the matrix. Then identify the system mission category for that confidentiality requirement. Finally, identify the firewall operating environment, either current or future. This should yield the level of robustness needed for the site's firewall. (Note: For details on how the case-specific architecture matrix was developed, see the definitions and processes supplied in the NSA DOD firewall guidance series (reference hhh) and Appendix A of the series.

(3) Step 3. Once the level of robustness is determined using the case-solution matrix, it can be mapped to the firewall functions matrix in Section 4.4, NSA DOD Firewall Guidance series (reference hhh) and the configuration guidance used to configure the site firewall.

d. The following paragraphs present an example of how a site would use this document to select a level of robustness applicable to the site's mission and configure the firewall using the guidance presented in NSA DOD firewall guidance series (reference hhh), Table 4.2.

(1) Situation. Site X wants to deploy a firewall between its local SBU LAN and the NIPRNET or Internet. Site X's LAN has 1,000 users, and they use the LAN to process information that is used to carry out normal daily business functions. The information processed on site X's LAN is not used to support deployed forces. Based on this information and the process described in paragraph 1c, determine the level of robustness required for site X's firewall, and determine which firewall functions will be allowed or denied on the firewall site X deploys.

(2) Solution - Step 1

(a) Using the process depicted above and in Figure C-K-A-1, identify site X's LAN as the enclave that needs protection.

(b) Determine site X's enclave confidentiality requirement is SBU, based on the information provided in the example description above.

C-K-A-3

Annex A  
Appendix K  
Enclosure C

**FOR OFFICIAL USE ONLY**

(c) Determine the system's mission category. To do this, use the system mission assurance category definitions found in Appendix A, Section A.1.2, and NSA DOD firewall guidance series (reference hhh), and the information provided in the example description above. Using the mission category and based on the fact that site X uses the LAN to carry out normal business functions and the processed information is not used to support deployed force, determine that site X's system mission category is MAC III.

(d) Finally, determine site X's operating environment to be LAN-to-WAN based on the fact that site X's 1,000-user network is considered a LAN, and the NIPRNET or Internet is considered a WAN.

(e) In summary from Step 1:

1. Site X's confidentiality requirement is SBU.
2. Site X's system mission category is MAC III.
3. Site X's operating environment is LAN-to-WAN (SBU connected to the NIPRNET or Internet).

(3) Solution -- Step 2

(a) With this information, use Table 4.1 in Section 4.3, NSA DOD firewall guidance series (reference hhh), to determine site X's required level of robustness. Table 4.1 is segmented based on confidentiality requirement or classification level (i.e., UNCLASSIFIED, SBU, and SECRET). Using Table 4.1, locate the SBU category.

(b) Once the SBU section is located in Table 4.1, identify the applicable SBU mission category, which in this case is administrative. Under the SBU, administrative section, locate the section for LAN-to-WAN. At this point, choose the description that best describes site X's LAN-to-WAN configuration, which in this case is SBU NIPRNET.

(c) Finally, following across the row that corresponds to SBU, administrative, LAN-to-WAN, SBU NIPRNET, determine that a firewall deployed by site X should have a medium level of robustness.

C-K-A-4

Annex A  
Appendix K  
Enclosure C

**FOR OFFICIAL USE ONLY**

(4) Solution -- Step 3. Using Table 4.2 in Section 4.4, NSA DOD firewall guidance series (reference hhh), identify the medium robustness column. Site X would then configure the firewall-specific functions to deny or allow based on the firewall function guidance recommended in the medium level of robustness column.

C-K-A-5

Annex A  
Appendix K  
Enclosure C

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

C-K-A-6

Annex A  
Appendix K  
Enclosure C

**FOR OFFICIAL USE ONLY**

APPENDIX L TO ENCLOSURE C  
PORTS AND PROTOCOLS MANAGEMENT PROCESS  
TO BE PUBLISHED

(INTENTIONALLY BLANK)



APPENDIX M TO ENCLOSURE C  
VIRTUAL PRIVATE NETWORKS  
TO BE PUBLISHED

(INTENTIONALLY BLANK)

## APPENDIX N TO ENCLOSURE C

## INTRUSION DETECTION SYSTEM

1. Description. The IDS is a complete system of components. An IDS monitors an information system for activity that may inappropriately affect the information system assets.

a. An IDS (inner circle) consists of sensors, scanners, and analyzers (Figure C-N-1). The IDS sensing environment (shaded perimeter) depicts the IDS observance and monitoring capability for information system activity and vulnerabilities. The IDS-derived information provides analysts at CERTs and NOSCs with technical event and incident data to process into intrusion analysis, correlation, and reporting. Figure C-N-1 is a graphical illustration of an IDS only. It does not intend to imply that sensors, scanners, and analyzers must be isolated, physical components.

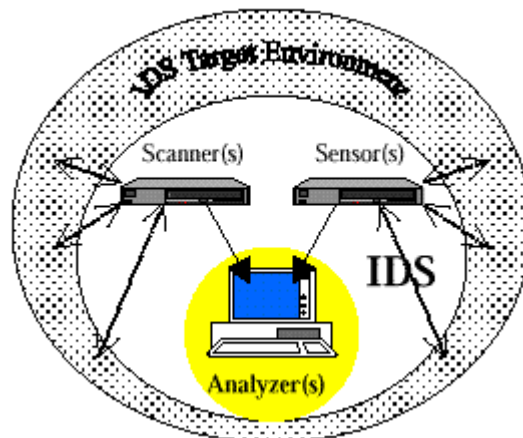


Figure C-N-1. Intrusion Detection System

(1) Sensors

(a) A sensor collects information indicative of an intrusion or inappropriate activity that may have resulted from misuse, access, or malicious activity of information system assets or the information itself.

(b) Sensors must be able to:

1. Collect data about selected events as they occur. Events may include authentication events, data-access events, configuration-access events,

service requests, network traffic, data introduction, and start-up and shutdown of audit functions.

2. Send all collected data to the analyzer for data reduction and analysis.

3. An IDS should operate in a “stealth” mode, which cannot be detected on the network via any conventional TCP/IP probing.

(2) Scanners

(a) A scanner collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion on an information system.

(b) Scanners must be able to:

1. Collect static configuration information about an information system. Configuration information may include detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities.

2. Forward all collected configuration information to an analytical facility (CERT, NOSC, etc.) for data reduction and analysis.

(3) Analyzer

(a) An analyzer accepts data from sensors and scanners and then applies analytical processes and information to derive conclusions about intrusions (past, present, and future). Response functions built into the analyzer determine what actions are taken. Possible actions range from a simple display of conclusions to an automated reconfiguration of the IT system or IDS to stop or prevent intrusions.

(b) An analyzer must be able to:

1. Receive data from identified sensors and scanners.

2. Process specified data to make intrusion and vulnerability determinations.

3. Respond to identified intrusions and vulnerabilities. Such responses may include report generation, visual signals and alarms, audible

signals and alarms, configuration changes, and/or invocation of remote warnings.

b. All IDS components must be able to:

(1) Protect themselves and their data from tampering.

(2) Be configured by an authorized user.

(3) Produce an audit trail (configuration changes, component and data accesses).

## 2. Information System and the IDS

a. All DOD information systems will deploy an IDS.

b. The IDS must be able to monitor itself as well as the information system.

c. IDSs can be utilized to monitor a computer system (not necessarily part of a larger network) or a computer network.

d. IDSs should also be kept updated with approved patches and/or upgrades, and regenerated or changed periodically to enhance their security.

e. IDSs should be acquired and configured in coordination with the C/S/A CERT or CERT equivalent.

## 3. Potential Attacks. Potential attacks can be directed against the IDS or the information system.

a. Attacks on the IDS by authorized and unauthorized users include:

(1) Attempts to compromise, disclose, destroy, or remove data collected by the IDS.

(2) Efforts to overwhelm or saturate the IDS by massive data overload causing the IDS to fail (distributed DOS).

(3) Misuse of the privileges available to an IDS (scanning for vulnerabilities and halting execution of information system resources).

(4) Attempts to halt or suspend the execution of the IDS.

(5) Misconfiguration of the IDS by authorized administrators.

(6) Attempts to modify the IDS configuration by unauthorized users.

b. Attacks by authorized and unauthorized users of the information system include:

(1) Inadvertent activities adversely affecting system assets (e.g., an administrator or user mistakenly granting a user write privileges to a file when the user is only allowed read privileges or mistaken deletion of data).

(2) Misuse of information system assets (users accessing forbidden web sites).

(3) Malicious activity (introducing a Trojan Horse or virus).

4. Considerations in Selecting an IDS. IDSs are configured to detect unauthorized intrusions through signatures or anomalous activity; however, some systems have better capabilities in some IDS requirements than others. Having one network-based IDS that is excellent at providing the best real-time alerts, and another that excels in providing good audit of the packet contents, will enhance the overall security response, incident handling and forensics. Joint IDS is available from DISA to provide after-the-fact auditing for analysis of the traffic. In addition, host-based intrusion detection adds further support to an overall defense-in-depth posture.

a. Collection Attributes

(1) Sensor programs separate from user interfaces to accommodate remote network traffic-sensor management.

(2) Recording of suspicious connections after signature-string anomaly detection, audit log monitoring , and detection on a configurable basis.

(3) Supports hierarchical alert-reporting topology.

b. Analysis Attributes

(1) Provide for a master database of signature strings that can be updated using system editor.

(2) Protect knowledge of specific signature strings to preclude attackers evading searched signature strings.

- (3) Provide for off-line and real-time analysis.
- (4) Prioritize analysis of suspicious activity by potential threat value (give human analyst a prioritized list to investigate).
- (5) Standardize report format.
- (6) Provide user-friendly alternatives for frequent alarms (eliminate rapidly scrolling screens and incomprehensible suspicious event overflows).
- (7) Provide user-friendly navigation from initial alarm of suspicious activity through stages of incident analysis.
- (8) Consolidate frequent reports of similar suspicious activity alarms.
- (9) Provide for analyst-configurable handling of suspicious activity alarms.
- (10) Incorporate state-of-the-art incident-tracking capabilities, database systems for storage and retrieval of incident reports, and graphical geographic attack-monitoring capabilities.

c. Management Attributes

- (1) General
  - (a) Provide for remote sensor management.
  - (b) Provide for remote operator access.
  - (c) Provide for authenticated access and encrypted data transfer between systems.
  - (d) Incorporate audio alarms.
  - (e) Provide remote alerts for unmanned operation.
  - (f) Perform routine data-gathering and configuration changes automatically by a centralized system in combination with other system automation utilities.
  - (g) Employ systems that do not require proprietary hardware.
  - (h) Employ reaction capabilities with proven limited self-damage.

(i) Employ expert systems for reducing the number of false alarms and improving detection of attacks.

(j) Log, retrieve, block, and recover from viruses and malicious code.

(2) Network IDS should have out-of-band management capabilities.

(3) Host IDSs should be transparent to the system on which they are installed and only minimally impact resources. Network IDSs should have minimal impact on network bandwidth.

#### 5. Minimum Security Functions and Requirements

a. Full IDS-access audit capability must be maintained, including normal SA access as well as any unauthorized-user activity.

b. The IDS must be able to identify and authenticate authorized users prior to allowing access to IDS functions and data.

c. IDS functions and data will be limited to and accessed only by authorized users.

d. The IDS must collect, store, and display and/or report intrusions and unauthorized activity.

e. The data collected, analyzed, or generated by the IDS must be protected from being compromised, destroyed, or disclosed.

f. All certificates, keys, passwords, or similar data used in authentication of authorized IDS users must be carefully protected from disclosure or compromise.

g. The IDS must be interoperable with other components of the IDS.

h. Confidentiality of data collected by the IDS must be maintained.

i. An IDS must have securely interoperable components.

j. An IDS must be interoperable with the information system it monitors.

k. Cryptographic components of the IDS must be FIPS-140-compliant.



6. Additional Information. Additional information on IDSs can be found in the IATF or at the IATF forum web site ([www.iatf.net](http://www.iatf.net)). Protection profiles for sensors, scanners, and analyzers can be found at [http://www.iatf.net/protection\\_profiles/intrusion.cfm](http://www.iatf.net/protection_profiles/intrusion.cfm).

(INTENTIONALLY BLANK)

## APPENDIX O TO ENCLOSURE C

## PUBLIC KEY MANAGEMENT

1. Public Key Infrastructure

a. PKI refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys.

b. The DOD PKI will support registration of users, dissemination of certificates, and a full range of certificate management services. This provides the critically needed support to individuals, applications, and network devices that provide secure encryption and authentication of network transactions as well as data integrity and non-repudiation.

c. Certificates are instruments used to convey trust. The DOD PKI will provide four types of certificates: identity certificates (used for authenticated access), E-mail signature certificates, key establishment (confidentiality) certificates, and object-signing certificates (used to sign mobile code). To achieve common certificates across the entire Department of Defense, the DOD PKI identity, E-mail signing, server (device), and encryption certificates will have a minimum/common set of attributes as specified in the certificate profile section of the DOD X.509 CP.

d. Public key technology provides the mechanisms to implement the following security services, which are available to individuals, network servers, network devices (e.g., routers and gateways), and properly configured software applications.

(1) Authentication. Mechanisms to strongly authenticate user identities and is a means to establish the validity of a claimed identity. The user's identity is verified as part of the certificate-issuing process (literally, the user is authenticated) and is bound to their certificate and private key by the CA.

(2) Confidentiality. Ability to enable strong encryption that can protect the privacy of information transferred during a transaction. Confidentiality is assurance that information is not disclosed to unauthorized persons, processes, or devices. Typically a public key exchange is used to establish a one-time session or message key. This key is encrypted using recipients' public keys to ensure that only valid recipients can decrypt the one-time key and in turn, decrypt the transaction.

(3) Integrity. Capability to ensure unauthorized party has not been modified transactions and the information is protected from undetected modification. Digital signatures can support data integrity verification. In contrast to handwritten signatures, verification of a digital signature both verifies the identity of the signer (authentication) and proves that the data remains unchanged (integrity). Note that authentication and integrity are both provided by the digital signature. In the case of signature-based integrity, authentication and integrity are inseparable.

(4) Non-repudiation. Ability to validate specific users involved in a transaction. Non-repudiation provides undeniable proof of a party's participation in a communication. Non-repudiation is defined as assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. Activities such as C2, official release of procurement documents, and travel reimbursement approvals are accompanied by legal requirements for non-repudiation. The Department of Defense intends to satisfy these legal requirements for non-repudiation by deploying digital signature technology and by supporting those mechanisms with the DOD PKI.

## 2. Public Key Certificates

a. Level of Assurance. The level of assurance associated with public key certificates is an assertion by a CA of the degree of confidence that a relying party may reasonably place in the binding of a subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on the proper registration of subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of the X.509 "Certificate Policy for the United States Department of Defense" (reference ggg). Personnel, physical, procedural, and technical security controls contribute to the assurance level of certification issued by a certificate management system

b. Factors in Determining Usage. The amount of reliance a program chooses to place on the certificate will be determined by various factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

c. Value of Information. This has been separated into importance of the information relative to the achievement of DOD goals and objectives, particularly the warfighter's combat mission and electronic commerce

applications. This includes the sensitivity of the information (classified or sensitive), criticality (mission categories; see Glossary) or monetary value for electronic commerce applications.

d. Threat Environment. Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering. Three items to consider when assessing the threat are its capability, risk tolerance, and access. DOD studies have concluded that a great majority of past compromises has involved insider threats.

e. Level of Environmental Protection. The DOD data networks on which PKI certificates will be used will have various levels of protection. Examples of mechanisms that provide network protection include network encryption, physical isolation, high assurance guards, and firewalls. These mechanisms are used to create a collection of system high networks and enclaves. The probability of external attack on protected networks is reduced because:

(1) Access is limited to people authorized to use the network and its interconnection points with other networks (the guards or firewalls), which eliminates anonymity.

(2) The lack of availability of hacker tools on the network hampers the capabilities of an attacker inside the network.

(3) The true amount of risk reduction associated with using these mitigation mechanisms can only be determined by a system security evaluation.

3. General Usage. DOD PKI strategy is based on five levels of assurance and guidance for their application. Guidance is based on the previous discussion of information value and environmental protection. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive by the Department of Defense, and information related to electronic financial transactions and other electronic commerce. The final selection of the security mechanisms and level of strength and assurance requires a risk-management process that addresses the specific mission and environment. The authority responsible for approving a specific level of assurance required for a particular implementation will vary from organization to organization, but will normally be the system accreditor acting in accordance with applicability guidance that follows:

a. DOD Class 2. This level is intended for applications handling unclassified information of low value in a minimally or moderately protected environment. DOD CAs will not issue class 2 certificates; the Department of Defense will issue class 3 and class 4 certificates exclusively. Access to DOD information resources will never be allowed on the basis of class 2 certificates. Class 2 certificates (or non-DOD-equivalent certificates) may be accepted by DOD parties for the purpose of authenticating or encrypting communication that does not access or process DOD information (meeting coordination, accessing web site information that has been cleared for unlimited distribution, etc.). These certificates may, for example, be issued by non-DOD commercial entities and used to authenticate communications with external vendors.

b. DOD Class 3. This level is intended for applications handling unclassified, medium-value information in moderately protected environments, unclassified high-value information in highly protected environments, and discretionary access control of classified information in highly protected environments.

c. DOD Class 3 Hardware. This level is intended for applications handling unclassified, medium-value information in minimally protected environments, unclassified, high-value information in moderately protected environments, and discretionary access control of classified information in highly protected environments. This level is also intended for all applications operating in environments appropriate for class 3 but which require a higher degree of assurance and technical nonrepudiation. This level is intended for applications performing contracting and contract modifications.

d. DOD Class 4. This level is intended for applications handling unclassified, high-value information (mission-critical, national security information) in minimally protected environments.

e. DOD Class 5. This level is intended for applications handling classified material in minimally protected environments and authentication of material that could affect the security of classified systems. Note: No current X.509 public key certificate implementation is approved for class 5 implementations. FORTEZZA cards currently provide this capability.

f. General Usage. The general usage is summarized in Table C-O-1. The levels of assurance listed are minimums. Any application that requires information to cross a classification boundary requires a class 4 assurance level.

Value of Information	Protection of Network Environment		
	High	Medium	Minimal
Low	CLASS 3	CLASS 3	CLASS 3
Medium	CLASS 3	CLASS 3	CLASS 3 Hardware
High	CLASS 3	CLASS 3 Hardware	Class 4

Table C-O-1. General Usage

4. Potential Attacks. Potential infrastructure attacks can be directed against users or the infrastructure (or information system itself).

a. Potential attacks against the infrastructure support to the user include:

- (1) Read traffic due to weak crypto (compromised or weak keys).
- (2) Masquerade (get a certificate with false information).
- (3) DOS (prevent signature from verifying; attack directories).
- (4) Insider intervention.

b. Potential attacks against the infrastructure include:

- (1) Violate trust model (generate an unauthorized cross-certification).
- (2) Acquire unauthorized certificate (insider or incorrect identification).
- (3) Force user to have weak key (known key or failed randomizer).
- (4) DOS (attack directories).
- (5) Compromise key during distribution.
- (6) Unauthorized access to data-recovery key.
- (7) Compromise PIN to gain access to user's private key (generation, distribution, and use).
- (8) Prevent user from determining compromise status during validation.
- (9) Substitute the attacker's public key for the users.

(10) Place malicious software into infrastructure elements.

5. PKI Authorities and Functions

a. The DOD Policy Management Authority (PMA) is a body established by the Department of Defense to:

(1) Oversee the creation and update of certificate policies, including evaluation of changes requested by DOD Services and Agencies, and plans for implementing any accepted changes; provide timely, responsive, DOD Service and Agency coordination to the Department of Defense.

(2) Review the CPS of DOD-operated CAs, registration authorities, local registration authorities (LRAs), and related certificate management authorities (CMAs) that offer to provide services to the Department of Defense by analyzing the CPS documents to ensure that the practices of the CMAs serving the Department of Defense comply with the DOD Certificate Policies.

(3) Review the results of compliance audits to determine if the CMAs are adequately meeting the stipulations of approved CPS documents, and make recommendations to these authorities and to the PMA regarding corrective actions or other measures that might be appropriate, such as revocation of CA certificates.

(4) Establish the suitability of non-DOD policies for use within the Department of Defense (for example, in cases where the technical mechanism of "policy mapping" is being considered).

(5) Offer recommendations to the DOD Program and Project Managers and DOD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the DOD certificate policies for specific applications.

b. The DOD PMA Signature Authority is the DOD CIO. The DOD PMA may delegate some of these responsibilities to a DOD PMA Implementation Authority. All elements of the DOD PKI and the DOD PKI subscribers are bound by this manual to comply with the DOD Certificate Policy, and with any applicable CPS as approved by the PMA.

c. The DOD PKI Certificate Policy Management Working Group (CPMWG) is chartered by the DOD PMA to:

(1) Create and update certificate policies, including evaluation of changes requested by DOD Services and Agencies, and plans for implementing



any accepted changes; provide timely, responsive, DOD Service and Agency coordination to the DOD certificate policy through a consensus-building process; report to DOD PMA on progress and deliverables.

(2) Work with C/S/A to craft CPS for DOD-operated CMAs that offer to provide services to the Department of Defense by analyzing the CPS documents to ensure that the practices of CAs serving the Department comply with the DOD Certificate Policies; report to DOD PMA on progress and deliverables.

(3) Coordinate CA compliance audits to determine if the CMAs are adequately meeting the stipulations of approved CPS documents, and make recommendations to the CAs and to the PMA regarding corrective actions or other measures that might be appropriate, such as revocation of CA certificates; report to DOD PMA on progress and deliverables.

d. The CA is an entity authorized by the PMA to create, sign, and issue public key certificates.

(1) The CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key.

(2) The CA is responsible for ensuring that all aspects of the services, operations, and infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of this policy.

(3) CA is an inclusive term, and includes all types of CAs. Any CA requirement expressed in this policy applies to all CA types unless expressly stated otherwise.

e. A registration authority is an entity that enters into an agreement with a CA to collect and verify subscribers' identity and information, which is to be entered into public key certificates. The registration authority must perform its functions in accordance with a CPS approved by the CA and the PMA.

f. Both CAs and registration authorities are CMAs. The DOD Certificate Policy will use the term "CMA" when a function may be assigned to either a CA or a registration authority, or when a requirement applies to both CAs and registration authorities. The term "registration authority" includes entities such as LRAs and verifying officials. The division of subscriber registration responsibilities between the CA and registration authority may vary among

25 March 2003

implementations of this certificate policy. This division of responsibilities shall be described in the CA's CPS.

g. CPS are required by the X.509, Certificate Policy for the United States Department of Defense (reference iii) before CAs, registration authorities, LRAs, or other CMAs are permitted to operate. The CPS describes how the PKI component will perform its functions to support the issuance and management of public key certificates. Each C/S/A element PKI component will operate in accordance with the CPS approved by the DOD X.509 PMA. The CPS outlines the PKI security requirements and required controls. It is the responsibility of the requesting activity to generate the CPS for the specific PKI component prior to operation of that component. To submit the CPS for evaluation, the CPMWG should be contacted at (410) 854 4900.

6. Additional Information. Additional information on PKI can be found in the, "X.509 Certificate Policy for the United States Department of Defense" (reference ggg), DISA web site <http://iase.disa.mil/policy.html> (PKI section) and IATF web site (<http://www.iatf.net>). The DOD PKI Program Management Office can be reached at (410) 854 4900.

APPENDIX P TO ENCLOSURE C  
SYSTEM SECURITY AUTHORIZATION AGREEMENT  
TO BE PUBLISHED

(INTENTIONALLY BLANK)

ENCLOSURE D

REFERENCES

- a. DOD 5200.2-R, Series, "Personnel Security Program"
- b. CJCSI 6510.01, Series, "Information Assurance (IA) and Computer Network Defense (CND)"
- c. CJCSI 6211.02, Series, "Defense Information System Network and Connected Systems"
- d. DOD Directive 5200.39, 10 September 1997, "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection"
- e. NSTISSI No. 7003, 13 December 1996, "Protected Distribution System"
- f. DOD Instruction 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation (C&A) Process"
- g. DOD Instruction O-8530.2, Series, "Support to Computer Network Defense (CND)"
- h. Executive Order 12958, 17 April 1995, "Classified National Security Information"
- i. DOD 5200.1-R, 14 January 1997, "Information Security Program"
- j. DOD 5500.7-R Change 4, 6 August 1998, "Joint Ethics Regulation"
- k. USD(P&R) and ASD(C3I) Memorandum, 29 June 1998, "Information Assurance (IA) Training and Certification"
- l. NSTISSD No. 500, 25 February 1993, "Information Systems Security (INFOSEC) Education, Training, and Awareness"
- m. NSTISSD No. 501, 16 November 1992, "National Training Program for Information Systems Security (INFOSEC) Professionals"
- n. NSTISSI No. 4013, August 1997, "National Training Standard For System Administrators in Information Systems Security (INFOSEC)"

25 March 2003

- o. National Institute of Standards and Technology (NIST) Special Publication 800-16, April 1998, "Information Technology Security Training Requirements"
- p. NSTISSI No. 4014, August 1997, "National Training Standard For Information Systems Security Officers (ISSO)"
- q. NSTISSI No. 4012, August 1997, "National Training Standard For Designated Approving Authority (DAA)"
- r. CJCSI 3402.01B, Series, "Alert System of the Chairman of the Joint Chiefs of Staff"
- s. DOD Directive O-8530.1 Series, "Computer Network Defense (CND)"
- t. NSTISSD No. 503, 30 August 1993, "Incident Response and Vulnerability Reporting for National Security Systems Security"
- u. DOD Instruction S-3600.2, 6 August 1998, "Information Operations (IO) Security Classification Guidance"
- v. DOD Directive 5105.61, 3 May 1997, "DOD Cover and Cover Support Activities"
- w. DOD Instruction 8500.2 Series, "Information Assurance (IA) Implementation"
- x. DI-2710-6-01, January 2001, "The Information Operations Threat To The Defense Information Systems Network (DISN)"
- y. National Disclosure Policy (NDP-1), 1 October 1988, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations"
- z. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"
- aa. DOD Directive 5230.20, 25 June 1984, "Control of Foreign Representatives"
- bb. DOD Directive 5230.25, 6 November 1984, "Withholding of Unclassified Technical Data from Public Disclosure"
- cc. DOD Instruction 5230.17, 17 August 1979, "Procedures and Standards for the Disclosure of Military Information to Foreign Activities"

25 March 2003

dd. CJCSI 5221.01, Series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

ee. CJCSI 6740.01, Series, "Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Nations"

ff. Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations (ITAR)"

gg. Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulations (EAR)"

hh. DOD Directive 5400.7, 29 September 1997, "DOD Freedom of Information Act Program"

ii. FIPS 10-4, April 1995, "Countries, Dependencies, Areas Of Special Sovereignty, And Their Principal Administrative Divisions"

jj. Title 10, United States Code, section 421

kk. NSTISSP No. 8, 13 February 1997, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments"

ll. DOD Instruction S-5225.1, Change 1, 4 November 1983, "Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations"

mm. CJCSI 6510.06 Series, "Communications Security Releases to Foreign Nations"

nn. DOD Directive C-5200.5, 21 April 1990, "Communications Security (COMSEC)"

oo. Public Law 100-235, 8 January 1988, "Computer Security Act of 1987"

pp. NSTISSAM INFOSEC 1-00, 8 February 2000, "Advisory Memorandum For The Use Of The Federal Information Processing Standards (FIPS) 140-1 Validated Cryptographic Modules In Protecting Unclassified National Security Systems"

25 March 2003

- qq. OMB Circular No. A-130, 28 November 2000, "Management of Federal Information Resources"
- rr. NCSC-1, 16 January 1981, "National Policy For Safeguarding And Control of Communications Security Material"
- ss. NCSC-2, 7 July 1983, National Policy on Release of Communications Security Information to US Contractors and Other US Nongovernmental Sources"
- tt. DOD Directive 4640.6, 26 June 1981, "Communications Security (COMSEC) Monitoring and Recording"
- uu. NTISSD No. 600, 10 April 1990, "Communications Security (COMSEC) Monitoring"
- vv. NSTISSP No. 3, 19 December 1998, "National Policy for Granting Access to US Classified Cryptographic Information"
- ww. Executive Order 12333, 4 December 1981, United States Intelligence Activities"
- xx. ASD(C3I) Memorandum, 16 January 1997, "Policy on Department of Defense Electronic Notice and Consent Banner"
- yy. Title 10, United States Code, section 2315
- zz. Title 15, United States Code, section 278g-3
- aaa. FIPS 140-2, 25 May 2001, "Security Requirements for Cryptographic Modules"
- bbb. DOD Directive 8500.1, Series, "Information Assurance (IA)"
- ccc. DOD 8510.1-M, Draft, "DITSCAP Implementation"
- ddd. Intelligence Community CIO, TOP SECRET/Sensitive Compartmented Information (SCI) and Below Interoperability Policy (TSABI)"
- eee. Director of Central Intelligence Directive (DCID) 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information within Information Systems"
- fff. National Security Agency "Department of Defense Firewall Guidance" Series



25 March 2003

ggg. DOD PKI Program Management Office, 31 May 2002, "X.509 Certificate Policy for the United States Department of Defense"

hhh. NSTISSI No. 4009, Revision 1, September 2000, "National Information Systems Security (INFOSEC) Glossary"

iii. Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms"

jjj. Federal Standard 1037C, 7 August 1996, "Telecommunications: Glossary of Telecommunications Terms"

kkk. Joint Publication 3-13, 9 October 1998, "Joint Doctrine for Information Operations"

(INTENTIONALLY BLANK)

## GLOSSARY

## PART I--ABBREVIATIONS AND ACRONYMS

ACL	access control list
ACERT	US Army computer emergency response team
AFCERT	US Air Force computer emergency response team
AOR	area of responsibility
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AUTODIN	automated digital network
B/P/C/S	base/post/camp/station
C2	command and control
CA	certification authority
CC	common criteria
CCII	commander's critical items of information
CDRUSSTRATCOM	Commander, United States Strategic Command
CERT	computer emergency response team
CI	counterintelligence
CIO	chief information officer
CIRT	computer incident response team
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CL	compliance level
CM	configuration management
CMA	certificate management authority
CMCS	communications security (COMSEC) material control system
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNSS	Committee on National Security Systems
COE	common operating environment
COMSEC	communications security
CONOPS	concept of operations
COTS	commercial-off-the-shelf
CPMWG	Certificate Policy Management Working Group
CPS	certification practice statement

C/S/A	combatant command, Service and/or agency
CWAN	coalition wide area network
D&D	denial and deception
DAA	designated approving authority
DCID	Director of Central Intelligence Directive
DECC	Defense Enterprise Computing Center
DES	data encryption standard
DIA	Defense Intelligence Agency
DICAST	Defense and Intelligence Community Accreditation Support Team
DII	defense information infrastructure
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DMS	Defense Message System
DMZ	demilitarized zone
DNS	domain name system
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOS	denial of service
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
DTG	date time group
EA	electronic attack
EAL	evaluation assurance level
EAR	export administration regulations
EO	executive order
EP	electronic protection
EW	electronic warfare
FDO	foreign disclosure officer
FIPS	federal information processing standard
FLO	foreign liaison officer
FMS	foreign military sales
FOUO	FOR OFFICIAL USE ONLY
FTP	file transfer protocol
GCCS	Global Command and Control System
GCSS	Global Combat Support System

GIAP	Global Information Grid (GIG) interconnection approval process
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
GSO	guarding solutions office
HTML	hypertext markup language
I&W	indications and warning
IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IATF	information assurance technical framework
IATO	interim authority to operate
IAVA	information assurance vulnerability alert
IAVB	information assurance vulnerability bulletin
IAVM	information assurance vulnerability management
IAW	in accordance with
IC	intelligence community
ID	identification
IDS	intrusion detection system
INFOCON	information operations conditions
INFOSEC	information systems security
INMS	integrated network management system
IO	information operations
IP	Internet protocol
IPC	information protection cell
IPSec	Internet protocol security
IRC	incident response center
ISP	Internet service provider
ISSM	information systems security manager
ISSO	information systems security officer
IT	information technology
ITAR	international traffic in arms regulations
IW	information warfare
J-3	operations directorate of a joint staff
J-6	command, control, communications, and computer systems directorate of a joint staff
JCMA	Joint Communications Security (COMSEC) Monitoring Activity
JP	joint publication
JTF	joint task force
JTF-CNO	Joint Task Force – Computer Network Operations

JULLS	Joint Universal Lessons-Learned System
JVAP	joint vulnerability assessment process
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LCC	local control center
LRA	local registration authority
MAC	mission assurance category
MARCERT	US Marine Corps computer emergency response team
MOA	memorandum of agreement
MOU	memorandum of understanding
MS-DOS	Microsoft Disk Operating System
NAT	network address translation
NAVCIRT	US Navy computer incident response team
NCC	network control center
NCSC	National Communications Security Committee
NDP	national disclosure policy
NIC	network interface cards
NIAP	national information assurance partnership
NIPC	National Infrastructure Protection Center
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOSC	network operations and security center
NSA	National Security Agency
NSISIP	National Security Information Systems Incident Program
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OCIN	organization's classified information network
OMB	Office of Management and Budget
OPR	office of primary responsibility
OPREP	operational report
OPSEC	operations security

OS	operating system
OSI	open systems interconnection
OUNET	organization's unclassified network
PDS	protected distribution system
PIN	personal identification number
PKI	public key infrastructure
PM	program manager
PMA	policy management authority
PNA	protection for the network
POC	point of contact
PSYOP	psychological operations
QoS	quality of service
RA	release authority
RASP	remote access security program
RCERT	regional computer emergency response team
RDT&E	research, development, test, and evaluation
RF	radio frequency
RHR	reliable human review
RI	referenced implementation
RNOSC	regional network operations and security center
RTO	request to operate
SA	system administrator
SABI	SECRET and Below Interoperability
SBU	sensitive but unclassified
SCAO	SIPRNET Connection Approval Office
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
SIGINT	signals intelligence
S/MIME	secure multipurpose internet mail extension
SMTP	simple message transfer protocol
SOP	standing operating procedure
SSAA	system security authorization agreement
SSES	system security engineering survey
SSH	secure socket shell
SSL	secure sockets layer
SSN	social security number
STIG	security technical implementation guide
SYN	synchronous idle character
TA	technical advisory

TBP	to be published
TCP	transmission control protocol
TLS	transport layer security
TSABI	TOP SECRET/SCI and Below Interoperability
UNIX	universal interactive executive
URL	universal resource locator
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USG	United States Government
USSTRATCOM	United States Strategic Command
VAT	vulnerability assessment team
VCTS	vulnerability compliance tracking system
VMS	vulnerability management system
VPN	virtual private networks
WAN	wide area network
WMD	weapons of mass destruction
WSH	windows scripting host
ZULU	time zone indicator for Universal Time



## GLOSSARY

## PART II--DEFINITIONS

access. Opportunity to make use of an information system resource. [NSTISSI No. 4009 reference hhh]

access control. Limiting access to information system resources only to authorized users, programs, processes, or other systems. [NSTISSI No. 4009 reference hhh]

accountability. Process allowing auditing of information system activities to be traced to a source that may then be held responsible. [NSTISSI No. 4009 reference hhh]

accreditation. Formal declaration by a DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NSTISSI No. 4009 reference hhh]

action. A step taken by a user or process in order to achieve a result, such as to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify, or delete. [CJCSI 6510.01 reference b)

application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs (DODD 8500.1 reference bbb)

architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Includes computers, ancillary equipment, and services, including support services and related resources. [DODI 5200.40 reference e]

asset. Any device on any DOD-owned or controlled information system network, to include but not limited to workstations, servers, routing devices (router, switch, firewall), networked peripherals (e.g., network printers) and guards. The device is considered a single node on a network, such that it has its own network identification (IP and/or media access control address).

audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NSTISSI No. 4009 reference hhh]

audit trail. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an information system to message routing in a communications system, or to the transfer of COMSEC material. [NSTISSI No. 4009 reference hhh]

authentication. 1. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. 2. A means of identifying individuals and verifying their eligibility to receive specific categories of information. 3. Evidence by proper signature or seal that a document is genuine and official. 4. In evasion and recovery operations, the process whereby the identity of an evader is confirmed. [JP 1-02 reference iii]

availability. Timely, reliable access to data and information services for authorized users. [NSTISSI No. 4009 reference hhh]

backup. Copy of files and programs made to facilitate recovery, if necessary. [NSTISSI No. 4009 reference hhh]

Blue Team. Cooperative effort by an interdisciplinary team to review, assess, and document vulnerabilities as a means to improve the security posture of information systems.

category. Restrictive label applied to classified or unclassified information to limit access. [NSTISSI No. 4009 reference hhh]

certification. Comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NSTISSI No. 4009 reference hhh]

classified information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. [JP 1-02 reference iii]

command and control system. The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing,

and controlling operations of assigned forces pursuant to the missions assigned. [JP 1-02 reference iii]

Command Communications Service Designators. An eight character alphanumeric that is used to identify the circuit throughout the joint communications network.

common operating environment (COE). The collection of standards, specifications and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces, runtime environment definitions, reference implementations, and methodology that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product.

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of COMSEC materials and information. a. **crypto-security** — The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. **transmission security** — The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. **emission security** — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems. d. **physical security** — The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. [JP 1-02 reference iii]

communications security monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications, including voice and data, to provide material for analysis in order to determine the degree of security being provided to those transmissions. [modified from NTISSD No. 600 reference uu]

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population. (DODD 8500.1 reference bbb)

computer emergency response team(s). Computer emergency response teams (CERTs) are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs as an operational organization for rapid response to both deployed and installation based Service forces. [JP 3-13 reference mmm] Note: CERT is an organization chartered by an information systems owner to coordinate or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. [JP 1-02 reference iii]

computer network exploitation. Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations. [CJCSI 6510.01 reference b]

computer network defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces, and other US Government agencies. [DOD Directive 8530.1, reference s]

Computer Network Defense (CND) Operational Hierarchy. The way the Department of Defense is organized to conduct CND. The Department is organized into three tiers to conduct CND. Tier One provides DOD-wide CND operational direction or support to all DOD Components. Tier Two provides

DOD Component-wide operational direction or support and responds to direction from Tier One. Tier Three provides local operational direction or support and responds to direction from a designated Tier Two entity. Tier One entities include the US Space Command and supporting entities such as the CND Service Certification Authorities, the Defense Criminal Investigative Organization Law Enforcement and Counterintelligence Center, and the National Security Incident Response Center. Tier Two includes CND Service providers designated by heads of components to coordinate component-wide CND. Tier Three includes all entities responding to direction from DOD Component Tier Two CND Service (e.g., local control centers that manage and control information systems, networks and services, either deployed or fixed at DOD Installations). (CJCSI 6510.01, reference b)

concept of operations. Document detailing the method, act, process, or effect of using an information system. [NSTISSI No. 4009 reference hhh]

confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices. [NSTISSI No. 4009 reference hhh]

configuration management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life-cycle of the information technology. [DODI 5200.40 reference f]

connection approval. Formal authorization to interconnect information systems. (DODD 8500.1 reference bbb)

contingency plan. Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. [NSTISSI No. 4009 reference hhh]

continuity of operations plan. The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. [JP 1-02 reference iii]

controlled interface. A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system) (DCID 6/3 reference eee).

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. [JP 1-02 reference iii]

controlled access protection. The command and control level of protection described in the Trusted Computer System Evaluation Criteria (Orange Book). Its major characteristics are: individual accountability, audit, access control, and object reuse. [NSTISSI No. 4009 reference hhh]

controlled unclassified information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes US information that is determined to be exempt from public disclosure in accordance with DOD Directives 5230.25 (reference bb) and 5400.7 (reference hh) or that is subject to export controls in accordance with the international traffic in arms regulations (reference ff) or the export administration regulations (reference gg).

criticality. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing.

cryptographic information. All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial. [JP 1-02 reference iii]

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. [JP 1-02 reference iii]

data integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [NSTISSI No. 4009 reference hhh]

defense critical infrastructures. Those physical and cyber-based systems and assets essential to mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy.

defense-in-depth. The DOD approach for establishing an adequate information assurance (IA) posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among information technology assets; and the selection of IA solutions based on their relative level of robustness. (DODD 8500.1 reference bbb)

defense information infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The DII connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. [JP 1-02 reference iii]

Defense Information Systems Network. The DOD consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. (DODD 8500.1 reference bbb)

denial of service (attack). Result of any action or series of actions that prevents any part of an information system from functioning. (NSTISSI No. 4009 reference hhh)

DOD Information Technology Security Certification and Accreditation Process. The standard DOD process for identifying information security requirements, providing security solutions, and managing information system security activities. [DOD 5200.40 reference f]

designated approving authority. Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority. [NSTISSI No. 4009 reference hhh]

designated disclosure authority (DDA). An official, designated by the head of a DOD component or by that DOD component's principal disclosure authority, who has been delegated disclosure authority in accordance with DOD Directive 5230.11, to control disclosures by subordinate commands or staff elements of classified military information to foreign governments and their nationals and to international organizations. (DOD Directive 5230.20 reference aa)

digital signature. Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Same as electronic signature. [NSTISSI No. 4009 reference hhh]

Discretionary Access Control (DAC). A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (DODI 8500.2 reference w)

electronic messaging services. Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business. [NSTISSI No. 4009 reference hhh]

electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. [JP 1-02 reference iii]

electronic surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. [NTISSD No. 600 reference uu]

emissions security. Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto equipment or an information system. [NSTISSI No. 4009 reference hhh]

enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the automated information systems applications or outsourced information technology-based processes they support, and derive their security needs from those systems. They provide standard information assurance capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic



mail. Enclaves are analogous to general support systems as defined in OMB A-130. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DODI 8500.2 reference w)

enclave boundary. The point at which an enclave's internal network service layer connects to an external network's service layer. (DODI 8500.2 reference w)

encryption. To convert plain text into unintelligible forms by means of a cryptosystem. (Note: The term "encrypt" covers the meanings of "encipher" and "encode.") [JP 1-02 reference iii]

evaluated products list (EPL). Equipment, hardware, software, and/or firmware evaluated by the National Communications Security Committee in accordance with DOD trusted computer system evaluation criteria and found to be technically compliant at a particular level of trust. The EPL is included in the National Security Agency Information Systems Security Products and Services Catalogue. [NSTISSI No. 4009 reference hhh]

event. 1. Occurrence, not yet assessed, that may effect the performance of an information system. (NSTISSI No. 4009, reference jjj) 2. Any suspicious occurrence affecting an information system. (CJCSI 6510.01, reference b)

External Certificate Authority (ECA). An external (outside DOD) agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DOD entities. Operating requirements for ECAs must be approved by the DOD Chief Information Officer, in coordination with the DOD Comptroller and the OSD General Counsel.

firewall. System designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both. [NSTISSI No. 4009 reference hhh]

foreign exchange personnel. Military or civilian officials of a foreign defense establishment (i.e., a DOD equivalent) who are assigned to a DOD component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DOD component. (DODD 5230.20 reference aa)

foreign liaison officer (FLO). A foreign government military member or civilian employee who is authorized by his or her government, and is certified by a DOD component, to act as an official representative of that government in its dealings with a DOD Component in connection with programs, projects, or agreements of interest to the governments. There are three types of FLOs:

a. Security Assistance. A foreign government representative who is assigned to a DOD Component or contractor facility pursuant to a requirement that is described in a Foreign Military Sales Letter of Offer and Acceptance.

b. Operational. A foreign government representative who is assigned to a DOD component pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education.

c. National Representative. A foreign government representative who is assigned to his or her national embassy or legation in Washington, D.C. (e.g., an attaché), to conduct liaison activities with the Department of Defense and the DOD components. (DODD 5230.20 reference aa)

foreign national. A person who is not a citizen or national of the United States. (DODD 5230.20 reference aa)

formal access approval. Documented approval by a data owner allowing access to a particular category of information. [NSTISSI No. 4009 reference hhh]

freeware. Also known as free software. Software that is free from licensing fees and has no restrictions on use; it can be freely copied, redistributed, or modified. [DOD CIO G&P Guidance Memorandum reference x) Note: Users must comply with regulatory procedures concerning the introduction of freeware onto DOD information systems.

functional domain. An identifiable DOD functional mission area. For purposes of this policy memorandum, the functional domains are: command and control, space, information operations, weapon systems, communications and broadcast, navigation, modeling and simulation, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and intelligence, surveillance, and reconnaissance.

Global Information Grid (GIG). Globally interconnected, end-to-end of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated

services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalitions, allied and non-DOD users and systems. Non GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

3. Processes data or information for use by other equipment, software, and services. (DODI 8500.2 reference w)

guards. Process limiting the exchange of information between systems. [NSTISSI No. 4009 reference hhh]

high-risk environment. Specific location or geographic area where there are insufficient friendly security forces to ensure the safeguarding of information systems security equipment. (NSTISSI No. 4009 reference hhh)

Intelligence Community member. Agencies, departments, or organizations that produce, process, handle, transfer, and receive intelligence information.

incident.

- a. An attempted entry, unauthorized entry, and/or an information attack on an information system.

- b. Information system-assessed occurrence having actual or potentially adverse effects on an information system. (NSTISSI No. 4009 reference ddd). (COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 USC 2315. [NSTISSI No. 4009 reference hhh]

identification. Process an information system uses to recognize an entity. (NSTISSI No. 4009 reference hhh).

information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (DODI 8500.2 reference w)

information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Note: This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [DODI 8500.2 reference w]

information assurance control. An objective information assurance condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. (DODI 8500.2 reference w)

information system security engineering. An engineering process that captures and refines information protection requirements and ensures their integration into information technology acquisition processes through purposeful security design or configuration. (DODI 8500.2 reference w)

Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying combatant commands, Services, and agencies (C/S/As) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself. [JP 1-02 reference iii]

information operations condition (INFOCON). INFOCON is a defense posture and response system for DOD information systems and networks. Note: INFOCON levels are: NORMAL – Normal readiness of DOD information systems and networks. ALPHA – Increased intelligence watch and strengthened security measures of DOD information systems and networks. BRAVO – A further increase in computer network defense (CND) force readiness above that required for normal readiness. CHARLIE – A further increase in CND force readiness but less than maximum CND force readiness. DELTA – Maximum

CND force readiness. [CJCSI 6510.01 reference b]

information producer. A person, group, or organization that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions. [DOD CIO G&P Guidance Memorandum reference x)

information system. The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. [NSTISSI No. 4009 reference jjj]

information assurance manager. The individual responsible for the information assurance program of a DOD information system or organization. While the term “information assurance manager” is favored within the Department of Defense, it may be used interchangeably with the information assurance title “information systems security manager.” [Draft DODI 8500.2 reference w]

information assurance officer. An individual responsible to the information assurance (IA) manager for ensuring the appropriate operational IA posture is maintained for a DOD information system or organization. While the term “information assurance officer” is favored within the Department of Defense, it may be used interchangeably with other IA titles, e.g., “information systems security officer,” “information systems security custodian,” “network security officer,” or “terminal area security officer.” [Draft DODI 8500.2 reference w]

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same. [JP 1-02 reference iii]

integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. [NSTISSI No. 4009 reference hhh]

intelligence community information. Sensitive compartmented information and any other information that is classified pursuant to section 1.5(c) of Executive Order 12958 and also bears special intelligence handling markings found in the “Authorized Classification and Control Markings Registry” maintained by the Community Management Staff.

interconnected. An interconnected information is composed of **separately accredited** information systems (i.e., Enclaves). Each self-contained information system maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating information system has its own information assurance office.

intrusion. 1. The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. [JP 1-02) 2. (For computers) Unauthorized access to an information system. (CJCSI 6510.01 reference b)

joint vulnerability assessment process. Process including evaluation and development of automated tools for measuring system risks that are operated by the National Security Agency and Defense Information Systems Agency against SECRET and Below Interoperability connection implementations to ensure Global Information Grid integrity.

layered defense. A combination of security services, software and hardware, infrastructures, and processes that are implemented to achieve a required level of protection. These mechanisms are additive in nature, with the minimum protection being provided by the network and infrastructure layers.

level of concern. A rating assigned to an information system that indicates the extent to which protective measures, techniques, and procedures must be applied. The Department of Defense has three levels of concern: a. High — Information systems that require the most stringent protection measures and rigorous countermeasures. b. Medium — Information systems that require layering of additional safeguards above the DOD minimum standard (Basic). c. Basic — Information systems that require implementation of the DOD minimum standard.

level of robustness. The characterization of the strength of a security function, mechanism, service, or solution, and the assurance (or confidence) that it is implemented and functioning correctly to support the level of concern assigned to a particular information system. The Department of Defense has three levels of robustness: a. High — Security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures. b. Medium — Security services and mechanisms that provide for layering of additional safeguards above the DOD minimum (LB) (Basic). c. Basic — Security services and mechanisms that equate to good commercial practices.

local area network (LAN). A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be

connected to one. Note 1: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. Note 2: An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network. An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN). Note 3: LANs are not subject to public telecommunications regulations. [Federal Standard 1037C reference jjj]

malicious logic. Hardware, software, or firmware capable of performing an unauthorized function on an information system. [NSTISSI No. 4009 reference hhh]

Memorandum of Agreement (MOA). A written agreement among the designated approving authorities (DAAs) responsible for the information processed and maintained by an information system (or collection of systems). The MOA stipulates all of the terms and conditions of the security arrangements that will govern the operation of the information system(s). The MOA shall include at least: (1) a general description of the information to be offered by each participating DAA; and (2) a discussion of all of the security details pertinent to the exchange of information between the DAAs. A lead DAA and description of the types of information services provided will be in the MOA to cover interconnected network of information systems under the purview of different DAAs. If no lead DAA is named, then both parties share responsibility.

mission assurance category (MAC). Applicable to DOD information systems, the MAC reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

1. MAC I. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

2. MAC II. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II

systems require additional safeguards beyond best practices to ensure assurance.

3. MAC III. Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices. [DODI 8500.2 reference y)

Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. (DODI 8500.2 reference w)

National Information Assurance Partnership. Joint initiative between the National Security Agency and the National Institute of Standards and Technology for security testing needs of both information technology (IT) consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. (DODI 8500.2 reference w)

national information infrastructure (NII). The NII is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. Although the NII is being designed, built, owned, operated, and used by the private sector, the government makes significant use of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks.

national security systems. Any telecommunications or information system operated by the US Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (40 USC 1452, Information Technology Management Reform Act of 1996.) [NSTISSI No. 4009 reference hhh]



network. Information system implemented with a collection of interconnected network nodes. [NSTISSI No. 4009 reference hhh]

network architecture. 1. The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. 2. The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use. [Federal Standard 1037C reference jjj]

nonpublic communication. A communication in which the parties thereto have a reasonable expectation of privacy. [NTISSD No. 600 reference uu]

non-repudiation. The assurance a sender of data is provided with proof of receipt and the recipient is provided with proof the message originated with the specified sender so neither can later deny taking part in the transaction. [NSTISSI No. 4009 reference hhh]

Non-classified Internet Protocol Routing Network (NIPRNET). Unclassified but sensitive Internet Protocol Network, one of two types of Internet Protocol routers owned by the Defense Information System Network. [DOD Chief Information Officer Annual Information Assurance Report Fiscal Year 2000] Note: The NIPRNET contains sensitive information and controlled information that must be protected. See definitions of controlled unclassified information and sensitive information.

operating system. An integrated collection of routines that service the sequencing and processing of programs by a computer. Note: An operating system may provide many services, such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware. [Federal Standard 1037C reference jjj]

operational threat environment. A generalized overview of the operational, physical and technological environment in which the system will have to function during its lifetime. Developments and trends that can be expected to affect mission capability during the system's life span should be included. Areas to be covered should include all generations of threat as outlined by a US Command.

1. Threats, first generation: Common hacker tools and techniques used in a non-sophisticated manner. Lone or possibly small groups of amateurs without large resources.

2. Threats, second generation: Non state-sponsored espionage or data theft. Common tools used in a sophisticated manner. Individuals or small groups supported by resources of a business, criminal syndicate or other trans-national group, including terrorists.

3. Threats, third generation: State-sponsored espionage. More sophisticated threat (than first and second) supported by institutional processes and significant resources. (CJCSI 6510.01, reference b)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [JP 1-02 reference iii]

password. Protected/private alphanumeric string used to authenticate an identity or to authorize access to data. [NSTISSI No. 4009 reference hhh]

physical security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. [JP 1-02 reference iii]

protect/protection philosophy. Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy. [NSTISSI No. 4009 reference hhh]

Protection Level. An indication of the implicit level of trust that is placed in a system's technical capabilities. A Protection Level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the information system without manual intervention and reliable human review (DCID 6/3 reference eee).

protected distribution systems. Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control. NSTISSI No. 4009 reference hhh]

Public Key Infrastructure. Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. [NSTISSI No. 4009 reference hhh]

purging. Rendering stored information unrecoverable by laboratory attack. [NSTISSI No. 4009 reference hhh]

push only technology. The means by which data is presented to a user without a specific action initiated by that user. In client-server terminology, the server initiates, or “pushes,” the data to the client, usually in accordance with a pre-established user profile. This interest profile typically contains information categories of interests (e.g., weather forecasts, stock quotes).

push/pull technology. A combination of technologies for information dissemination and retrieval. Traditionally, data is retrieved by a user request, such as by a Web user. In this case, the user “pulls” information. Alternatively, an information server may “push” information to the client without client intervention, usually by applying a predefined profile that filters information.

react/real time reaction. Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access. [NSTISSI No. 4009 reference hhh]

red team. Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems. [NSTISSI No. 4009 reference hhh]

reliable human review. Any manual, automated, or combined process or procedure for opening and reviewing digital objects (e.g., files, images) to ensure that the digital object can be transferred across a controlled interface.

remote access. Enclave-level access for authorized users that are external to the enclave that is established through a controlled access point at the enclave boundary. (DODI 8500.2 reference w)

remote diagnostics/maintenance. The operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system) remote service for analysis or maintenance.

risk analysis. Probability and severity of loss linked to hazards. (JP 1-02 reference iii)

risk assessment. Process of analyzing threats to and vulnerabilities of an information system and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. [NSTISSI No. 4009 reference hhh]

risk index. Difference between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g., classification and categories) of data processed by the system. [NSTISSI No. 4009 reference hhh]

risk management. 1. A process by which decision-makers eliminate, reduce, offset or accept risk. [Critical Infrastructure Protection definition] 2. Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. [NSTISSI No. 4009 reference hhh]

router. In data communications, a functional unit used to interconnect two or more networks. Note 1: Routers operate at the network layer (layer 3) of the ISO Open Systems Interconnection—Reference Model. Note 2: The router reads the network layer address of all packets transmitted by a network, and forwards only those addressed to another network. [Federal Standard 1037C reference jjj]

SECRET and Below Interoperability. An Assistant to the Secretary of Defense (Command, Control, Communications, and Intelligence)-directed, Joint Chiefs of Staff-sponsored, National Security Agency/Defense Information Systems Agency-executed initiative to enhance SECRET and Below Interoperability, measure community risk, and protect the Global Information Grid information systems infrastructure.

SECRET Internet Protocol Router Network. Worldwide SECRET level packet switch network that uses high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry. [JP 1-02 reference iii]

security domain. Refers to a discrete information system identified by its authorized classification level and releasability, and administrative controls. It does not refer to information systems interconnection of compartments at the same classification level. Manual transfer processes or controlled interfaces are required to transfer information between security domains that operate under different security policies.

security incident. An attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or

denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code [NSTISSD 503 reference t]. (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.)

security incident response. Actions conducted to resolve information systems security incidents and protect national security systems. [NSTISSD 503 reference t]

security label. A piece of information that represents the hierarchical classification (CONFIDENTIAL, SECRET, or TOP SECRET) and non-hierarchical compartments (e.g., specific sensitive compartmented information or special access program controls) of a subject or object and that thus describes the sensitivity of the data in the subject or object. Security labels are used as the basis for mandatory access control.

security markings. Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions. For DOE information, these could include indicators of information type (such as Restricted Data), and Sigma categories (DCID 6/3 reference eee)

security penetration testing. System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain “root” or “superuser” privileges) by exploiting flaws in system design or implementation.

security safeguards. Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See accreditation. [NSTISSI No. 4009 reference hhh]

security support structure. Those components of a system (hardware, firmware, software, data, interfaces, storage media, and communications media) that are essential to the enforcement of the system’s security policies.

Security Technical Implementation Guide. A guide for information security. A compendium of security regulations and best practices from many sources that apply to an operating system or a part of the GIG infrastructure.

sensitive compartmented information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

sensitive information. Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987.") Examples of sensitive information include, but are not limited to information in DOD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following:

1. For Official Use Only (FOUO). In accordance with DOD 5400.7-R, DOD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA).
2. Privacy Data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 U.S.C. 552a) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.
3. DOD Unclassified Controlled Nuclear Information (DOD UCNI). Unclassified Information on security measures (including security plans, procedures, and equipment) for the physical protection of DOD Special Nuclear Material (SNM), equipment, or facilities in accordance with DOD Directive 5210.83. Information is designated DOD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities.
4. Unclassified Technical Data. Data that is not classified but is subject to export control and is withheld from public disclosure according to DOD Directive 5230.25.
5. Proprietary Information. Information that is provided by a source or sources under the condition that it not be released to other sources.

6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with DOD 5200.1-R.

7. Department of State Sensitive But Unclassified (DoS SBU). Information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security policies.

8. Drug Enforcement Administration (DEA) Sensitive Information. Information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

special enclave network. DOD information systems and/or computer networks with special security requirements (e.g. special access program, special access requirements, and designated as special enclave by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). (DOD Instruction O-8530.2 reference g)

strong authentication. A form of authentication whereby it is very difficult or impossible for a hostile user to successfully intercept and employ a transmitted authenticator (i.e., highly resistant to replay attack).

strong binding. A mechanism that provides an explicit link (e.g., cryptographic association) between an end entity (e.g., individual user, author, reliable human reviewer) and data. The binding provides traceability (proof of origin, attribution, non-repudiation capability) of the data to the end entity. The binding (integrity seal) is also used to detect unauthorized modification of or tampering with the data. An example of a strong binding is a cryptographic digital signature.

susceptibility. Technical characteristics describing inherent limitations of a system that have potential for exploitation.

survivability. The ability of a computer and/or communications system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.

system administrator. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of

established information security policy and procedures. [NSTISSI No. 4009 reference hhh]

system high security mode. Information system (IS) security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an IS; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and c. valid need-to-know for some of the information contained within the IS. [NSTISSI No. 4009 reference hhh]

target. A computer or network logical entity (account, process, or data) or physical entity (component, computer, network or internet network). (CJCSI 6510.01, reference b)

technical vulnerability. A hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or denial of service. [NSTISSD 503 reference t]

technique. A means of exploiting a computer or network vulnerability. (CJCSI 6510.01, reference b)

telecommunications. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. [NSTISSI No. 4009 reference hhh]

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated information-processing equipment; these investigations are conducted in support of emanations and emissions security. [JP 1-02 reference iii]

threat. Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [NSTISSI No. 4009 reference hhh]

transmission security. Component of communications security resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. [NSTISSI No. 4009 reference hhh]



unauthorized result. An unauthorized consequence of an event. (CJCSI 6510.01, reference b)

US classified cryptographic information. 1. TOP SECRET and SECRET, CRYPTO designated, key and authenticators. 2. All cryptographic media that embody, describe, or implement classified cryptographic logic; this includes full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, cryptographic computer software, or any other media that may be specifically identified by the NSTISSC. (CJCSI 6510.01, reference b)

unclassified information. Information that has not been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. [NSTISSI No. 4009 reference hhh]

US nongovernmental source. An individual US citizen or a US corporation, association, or other organization substantially composed of US citizens, that is not directly a part of the US Government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding Active or Reserve military personnel, Civil Service employees, and other individuals employed directly by the Government); specifically excluded are corporations or associations under foreign ownership, control, and influence. [CJCSI 6510.01, reference b]

users. Person or process authorized to access an information system. [NSTISSI No. 4009 reference hhh]

virtual private network. Protected information system link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the user the impression a dedicated line exists between nodes. [NSTISSI No. 4009 reference hhh]

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02 reference iii)

vulnerability analysis. The systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [NSTISSI No. 4009 reference hhh]

vulnerability assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [NSTISSI No. 4009 reference hhh)